Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-101

Cyber Space and its Governance

Post Graduate Diploma in Cyber Law (PGDCL)

2020

Cyberspace and its Governance

Dr. Babasaheb Ambedkar Open University

Cyber Space and Its Governance

Course Writer

Dr. Peter Ladis F — Faculty, Chanakya Law University, Patna, Bihar

Mr. Kumar Gaurav — Faculty, Chanakya Law University, Patna, Bihar

Content Editors

Prof. (Dr.) Nilesh K. Modi — Professor & Director, School of Computer Science
Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. June 2020

This publication is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) https://creativecommons.org/licenses/by-nc-sa/4.0/

ISBN: 978-81-949119-3-7

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Cyber Space and Its Governance

Block-1: CYBERSPACE: MEANING AND ITS DEVELOPMENT

UNIT-1 CYBERSPACE – AN OVERVIEW OF THE CONCEPT 006

UNIT-2 INHERENT CHARACTERISTICS OF CYBERSPACE 015

UNIT-3 FORMS OF CYBERSPACE REGULATIONS 028

UNIT-4 IT CYBERSPACE REGULATORY THEORY OF LAWRENCE LESSIG 040

Block-2: FUNDAMENTALS OF CYBER LAW

UNIT-1 OUTLINE OF LEGISLATIVE FRAMEWORK FOR CYBER LAW 050

UNIT-2 HISTORY AND EMERGENCE OF CYBER LAW 062

UNIT-3 OUTREACH AND IMPACT OF CYBER LAW 075

UNIT-4 MAJOR AMENDMENTS IN VARIOUS STATUTES 086

Block-3: PERSONAL JURISDICTION IN CYBERSPACE

UNIT-1 ESTABLISHMENT OF PERSONAL JURISDICTION IN CYBERSPACE 098

UNIT-2 OVERVIEW OF TESTS AND INTERACTIVITY 109

UNIT-3 JURISDICTIONAL APPROACHES OF ONLINE CONTRACT 119

UNIT-4 BASIS OF JURISDICTION AND INDIAN APPROACH 129

Block-4: FREEDOM OF EXPRESSION IN CYBERSPACE

UNIT-1 INDIAN CONSTITUTION AND FREEDOM OF EXPRESSION 139

UNIT-2 EXAMINATION OF RIGHTS UNDER INDIAN LAWS 148

UNIT-3 THE LEGISLATIVE RESPONSES IN CYBERSPACE 158

UNIT-4 NATIONAL SOVEREIGNTY AND FREEDOM OF EXPRESSION 170

Block-1
Cyberspace: Meaning and Its Development

Unit 1: Cyberspace-An Overview of the Concept

1

UNIT STRUCTURE

1.1. Learning Objectives

1.2. Introduction

1.3. Meaning and Definition of Cyberspace

1.4. Layers of Cyberspace

1.5. Cyberspace Vs. the Internet

1.6. Contemporary Issues of Cyberspace

1.7. Let's sum up

1.8. Check your progress: Possible Answers

1.9. Further Reading

1.10. Activity

1.1 LEARNING OBJECTIVES

After studying this unit, the student should be able to understand:

- The meaning of the concept called cyberspace and its different definitions.
- Get aware about different layers of cyberspace.
- The relationship of the cyberspace and the internet.
- Recent and contemporary developments of and in the cyberspace.

1.2. INTRODUCTION

Cyberspace is a unique domain that is operationally distinct from the other operational domains of land, sea, air, and space. It provides, through the Internet, the capability to create, transmit, manipulate, and use digital information. The digital information includes data, voice, video, and graphics transmitted over wired and wireless facilities between a wide range of devices that include computers, tablets, smartphones, and control systems. The Internet serves as the transport

mechanism for cyberspace. The extensive variety of content is attractive to hackers, criminal elements, and nation-states with the objective of disrupting commercial, military, and social activities.

1.3 MEANING AND DEFINITION OF THE CYBERSPACE

Oxford English Dictionary (1997): "The notional environment within which electronic communication occurs."

Merriam-Webster Third New International Dictionary (2002): "The on-line world of computer networks."

Cambridge Academic Content Dictionary: "an electronic system that allows computer user around the world to communicate with each other or to access information for any purpose."

Cyberspace has been in our lexicon for over two decades now. William Gibson used it to describe "a consensual hallucination" in his science fiction novel, *Neuromancer (1984):*, when he sought a name to describe his vision of a global computer network, linking all people, machines and sources of information in the world, and through which one could move or "navigate" as through a virtual space.

The word ***"cyber",*** apparently referring to the science of cybernetics, was well-chosen for this purpose, as it derives from the Greek verb ***"Kubernao",*** which means "to steer" and which is the root of our present word "to govern". It connotes both the idea of navigation through a space of electronic data, and of control which is achieved by manipulating those data.[1]

Cyberspace represents the new medium of communication, electronic communication, which is fast and replacing the more traditional methods of communication. The physical objects of traditional communication are being superseded by new electronic objects. Just as physical objects exists in physical space, so do these cyber objects exist in cyberspace.2Cyberspace is a metaphor because it identifies the region where electronic communication occurs as being a kind

of space. We can analyze it using the terminology of I. A. Richards: "vehicle" and "tenor." The vehicle, or actual term used for the metaphor, is a combination of the morphemes "Cyber" (a trade name for computers which has become generalizable to all things computer related) and "space" (which covers a lot of territory: outer-space, inner-space, euclidean-space, non-euclidean-space, and others). The tenor, or underlying situation referred to in the metaphor, is the strange but real region created within an electric network of telephones and computers. Author Bruce Sterling refers to cyberspace as not exactly "real," but being a genuine place where things happen with actual consequences. Careers are made in cyberspace, thieves' prowl in cyberspace; increasingly complete records of our lives are stored in cyberspace.[3]

1.4.LAYERS OF CYBERSPACE

In order to understand the concept of cyberspace, one way to do so is to conceptualize cyberspace in terms of multiple interdependent layers of activities. There are varied conceptualizations of the different numbers and names of layers present in current academic discourse. However, the four-layer model of cyberspace can be considered as the best way to define cyberspace.[4]

1. The Physical layer contains all the hardware devices, which include routers, switches, storage media, satellites, sensors, and other technical conduits, both wired and wireless. The physical infrastructure can be located geographically in "real space" and is thus subject to different national jurisdictions. If it were removed, the overlying layers would disappear as well, as happened in 2011 in Armenia, were reported 90% of all Internet services crashed due to a retired 75-year-old woman who single-handedly sliced through an underground fiber optic cable with her spade.

2. The Logical Layer generally refers to the code, which includes both the software and the protocols incorporated within that software. Generally speaking, a protocol defines the rules or conventions necessary to obtain a certain goal (e.g., communication). Formalizing a protocol makes it a standard. Software, in contrast, is the computer program that implements these

protocols. In this respect, protocols "are not considered to be satisfactory standards until interoperable independent implementations [within different computer programs] have been demonstrated. (This is the embodiment of the "running code" slogan.)" Networking protocols are commonly segmented by their function, and how close (or how far) away they work from the "end-user"—the average computer user. In the most common of segmentation, known as the OSI Model, basic everyday client-side applications (such as Windows Internet Explorer) operate at the top of the model (level 7), while the aforementioned TCP works on Level 4 (the Transport layer) and IP work on Level 3 (the Internet layer). Built upon the Web, for instance, more complex applications often combine certain aspects of services, which can be eventually combined and applied by other applications on even higher levels. This flexibility presents inexhaustible possibilities to create new services, which, today, include search engines, Weblog, social networking sites, podcasts, Internet telephony, Web mapping, etc.

3. The Content/Information Layer describes all the information created, captured, stored and processed within cyberspace. Information is defined as "knowledge concerning objects, such as facts, events, things, processes, or ideas". It contains all human-readable messages delivered by social media Websites or email; content of articles and books kept on memory sticks and virtual databases; news broadcasted via blogs and Websites; and music, movies and pictures consumed online. However, access to information can also be systematically limited. Blocking or removing online content from the Web happens for reasons such as protecting intellectual property rights, securing national order or social identity.

4. The Social Layer is made up of all the people using and shaping the character of cyberspace. It is the actual Internet of people and potential relationships, rather than the implied Internet of hardware and software. Essentially, the social layer includes governments as well as private sector, civil society and technical community actors. However, all share a specific characteristic: while in "real" life (extra cyberspace) people can ultimately be identified by their unique DNA code, attribution is much more difficult on the Net (intra cyberspace).[5]

1.5 CYBERSPACE VERSUS INTERNET

Cyberspace is nothing more than a symbolic and figurative space that exists within the scope of Internet. It can be said that anything that is done via the use of Internet, occurs within the confines of the cyber-space, whether that is sending an e-mail, a website, or playing a game, all of these things exist within the cyber-space.Internet, on the other hand, is a network of networks, what that means is that it is a global network that is creating by linking smaller networks of computers and servers. This network allows users to share information and other data from one point to another. The data can be in the form of text, image, or video.[6]

Cyberspace does not exist physically, except in the countless miles of electronic circuitry, fiber optic cables and silicon chips which make up our computers and our networks. Cyberspace, by its very nature, is everywhere and nowhere at once; it is the everythingness and nothingness of William Gibson's matrix. Cyberspace is an infinite, universal space, achieved by technology inhabiting a minimal amount of physical space.[7]

But immersive cyberspace as mediated through virtual interfaces, unlike the infinite reaches of physical space, is nothingness. It is a blank, black void until an artificial context is introduced. It is nothing, placeless and indescribable. The void of cyberspace has no gravity and no micro or macroclimate of Sun, wind, earth and water. In cyberspace even a horizon is artificial. There are no building codes, no monetary budgets and no neighbours in cyberspace.[8]

Internet is a network of networks, what that means is that it is a global network that is creating by linking smaller networks of computers and servers. Cyber-space is nothing more than a symbolic and figurative space that exists within the scope of Internet.There is a lot of confusion between the usage of the terms, Cyberspace and Internet. Many people think that the words mean the space, while others think that they mean two completely different things within the field of technology. The truth of the matter is that it is something in the middle. The terms do mean two different things, but the confusion arises due to the fact that these things are closely interrelated, due of which they are often mistakenly used interchangeably.[9]

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes since then. The origin of the Internet devised from the concept of Advanced Research Project Agency Network (ARPANET). ARPANET was developed by the United States Department of Defense. Basic purpose of ARPANET was to provide communication among the various bodies of government. Initially, there were only four nodes, formally called Hosts. In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as the Internet. By the time, with the invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripts languages etc. Internet provided a medium to publish and access information over the web.

Internet covers almost every aspect of life, one can think of. Let us discuss some of the advantages and disadvantages of the internet:

ADVANTAGES:

- The Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the web that uses the Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook
    - Twitter
    - Yahoo
    - Google+
    - Flickr
    - Orkut
- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
    - Online Television

- Online Games
- Songs
- Videos
- Social Networking Apps

- The Internet allows us to use many services like:
  - Internet Banking
  - Matrimonial Services
  - Online Shopping
  - Online Ticket Booking
  - Online Bill Payment
  - Data Sharing
  - E-mail

- The Internet provides the concept of **electronic commerce** that allows the business deals to be conducted on electronic systems.

DISADVANTAGES

- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is **Spamming**. Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of the entire system.
- **A virus** can easily be spread to the computers connected to the internet. Such virus attacks may cause your system to crash or your important data may get deleted.

- Also, the biggest threat on the internet is pornography. There are many pornographic sites that can be found, letting your children use the internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

From the above discussion it can be said that now internet is a social phenomenon that has transformed many aspects of daily life. However, one cannot separate the internet and cyberspace from each other, they cannot be independent of each other. Their interrelationship will further be elaborated in different chapters.

1.7. LET'S SUM UP

In this chapter we tried to explore the concept of cyberspace by first discussing the different definitions available. The term first appeared in the fiction novel which now represents a virtual place which is both real and artificial at the same time. With introduction of internet it can be said that it has opened new medium of communication, a global space inhabited everyday. To further understand the concept we discussed the four different layers of cyberspace and how these layers carried different framework and functions. We touched upon the numerous changes that took place regarding cyberspace till date. In brief we have discussed relationship of internet and cyberspace, how they supplement and complement each other. The characteristics of cyberspace will be discussed in the next chapter in order to have in-depth understanding of the concept of cyberspace.

1.8 FURTHER READING

- http://pespmc1.vub.ac.be/CYBSPACE.html
- https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSPExports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210
- https://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf

- See, for instance, Martin C. Libicki, *Conquest in Cyberspace. National Security and InformationWarfare*(Cambridge: Cambridge University Press, 2007). Chapter 10.; and Franklin D. Kramer, StuartH. Starr, and Larry Wentz, eds., *Cyber Power and National Security* (Washington, DC: NationalDefence UP, 2009), Chapter 2.
- https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html
- https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Q. 1 What do you understand by 'cyberspace'?

A. It is the virtual space that allows navigations for the purposes of electronic communication through a medium using computers, computer network and their users.

Q. 2 What are the various layers of cyberspace?

A. The various layers of cyberspace are i) Physical Layer, ii) Logical Layer, iii) Content Layer and iv) Social Layer.

Q. 3 What are the disadvantages associated with cyberspace?

A. The disadvantages associated with cyberspace *inter alia* include that it involves scope of spamming, virus infection, exposure to pornography, identity theft, etc.

Q. 4How is cyberspace different from the internet?

A. Cyberspace is different from the internet because while the former is the network of networks interlinking devices and servers, the former only forms a symbolic space which does not exist physically but figuratively forms a part of everything going on in the internet.

1.10 ACTIVITY

Write an essay on the concept of cyberspace with special focus on its emergence, growth and its comparison with the internet. (800 words)

Unit 2: Inherent Characteristics of Cyberspace

2

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Borderless
1.4 Anonymity
1.5 Types of anonymity
1.6 Speed
1.7 Interconnectedness
1.8 Surveillance
1.9 Let's sum up
1.10 Check your progress : Possible Answers
1.11 Further Reading
1.12 Activity

1.1 LEARNING OBJECTIVES

After studying this unit, the student should be able to understand:

- The inherent characteristics of cyberspace
- Impact of the borderless phenomenon on regulation
- Know the pros and cons of anonymity feature cyberspace
- Realization of challenges posed by the speed of cyberspace
- Analyse the significance of Interconnectedness and Surveillance feature of cyberspace.

1.2. INTRODUCTION

The Internet is the newest form of communication between organizations and people in modern society. Everyday commerce depends on it, and individuals use it for social interactions, as well

as for reference and learning. Discoveries, Inventions and spread of new Information Technologies brought about by computers, internet and cyberspace widen the scientific horizon but pose new challenges and created problems for the legal world in all aspects of the law. [10]Cyberspace provides opportunities for innovation, commerce, and societal advancement but also raises significant issues for policymakers in securing cyber vulnerabilities, ensuring privacy and protection of personal data, and considering the use of cyberweapons as a national security asset. Cyber threats pose a broad and deep challenge. Over the past decade, governmental and non-state hackers have become increasingly sophisticated in their assaults on the cyber systems the nation depends on essential services, economic prosperity, and security. [11]Such breaches threaten critical infrastructure, intellectual property, privacy of users' data, sensitive national security information, and government personnel data. Future cyber-attacks could threaten the interconnected global economy and raise the prospect of cyber warfare between nation-states. The Internet is also being used for other malign purposes—by criminals to operate their nefarious enterprises and by terrorists to recruit and encourage violent attacks through online propaganda. If we analyze the challenges then we come to know that seed of these complications lies in inherent characteristics of cyberspace i.e. cyberspace is a borderless phenomenon, a feature of anonymity in cyberspace, lightning speed of cyberspace and interconnectedness along with surveillance characteristics of cyberspace.

1.3. BORDERLESS

Cyberspace is a borderless phenomenon. It defies the geographical territories and that is why it has been said that in the regime of cyberspace geography became history. Distance is dead in cyberspace. In this web shrink world, anyone can visit any destination virtually. It turned the word in a small village which is interconnected through various computer networks distributed worldwide. This borderless phenomenon is a double-edged sword because this feature of cyberspace can be exploited by both a netizen as well as the cyber offender. This creates a serious threat to the jurisdictional aspect of cyberspace which is the most complex legal issue of cyberspace.In the cyberspace, there is no geographical boundary. It establishes immediate long-

[10] Neeta Pramod, 'A study of formation and challenges of electronic contract in Cyberspace' <http://www.legalservicesindia.com/article/1943/A-study-of-Formation-and-challenges-of-electronic-contract-in-cyberspace.html>

[11]MarttiLehto and PekkaNeittaanmäki , *Cyber Security: Power and Technology* (3rd Edition, Springer 2018) 334

distance communications with anyone who can have access to any website. [12]Jurisdiction is the authority of a court to hear a case and resolve a dispute. The issue of Jurisdiction is highly conflicting and debatable in cyberlaw as to the maintainability of any suit which has been filed. [13]It becomes more complicated largely on account of the fact that the internet is borderless. The notion of jurisdiction is rooted in territoriality from the point of view of both the court which can properly assert jurisdiction and from the point of view of the law that should be applied while deciding the dispute. [14]In domestic transactions, a court will always have the jurisdiction to enforce their respective laws within their physical, geographical and political boundaries but the enforcement issues throw up several challenges when it comes to international transactions due to constant change in technology in borderless cyberspace

1.4. ANONYMITY

Anonymitycan be defined simply as being without a name or with an unknown name.[15]***Pseudonymity***is the use of a false name. Anonymity is derived from the Greek word **ανωνυμία**, meaning without a name or name-less. In colloquial use, the term typically refers to a person and often means that the personal identity or personally identifiable information of that person is not known. [16]More strictly, and in reference to an arbitrary element (e.g. a human, an object, a computer), within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous". [17]

Anonymity in cyberspace is a major concern for the global community. The introduction, growth and utilisation of information and communication technologies (ICTs) have been accompanied by an increase in criminal activities. With respect to cyberspace, identities are easily cloaked in anonymity. [18]Once a message sender's identity is anonymous, cyberspace provides the means to

[12]SuneetDwivedi, 'Jurisdiction Issues in Cyber Crime' (AcademiaEdu, 20-07-2007) <https://www.academia.edu/3700800/CYBER_CRIME_JURISDICTION>
[13]Vakul Sharma, *Information Technology Law and Practice* (3rdEdn. 2011 Universal) 567
[14]SubhajitBasu, '*Policymaking, Technology and Privacy in India'*, 2010 Vol II Indian Journal of Law and Technology
[15]Seymour Bosworth, M EKabay and Eric, Computer Security Handbook – I (5TH EDN. 2009 Wiley) 778
[16]Ibid
[17]Jacob van Kokswijk, *Digital Ego: Social and Legal Aspects of Virtual Identity* (5thEdn. 2007 Eburon)
[18] Mohammed Chawki, '*Anonymity in Cyberspace: Finding the Balance between Privacy and Security'*, (Droit-Tic, Juill. 2006)<http://www.droit-tic.com/pdf/Anonymity_Cyberspace.pdf.>

perpetrate widespread criminal activity to the masses, with little chance of apprehension.[19] On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government enables entrepreneurs to acquire and share technical information without alerting their competitors and permits individuals to express their views online without fear of reprisals and public hostility. [20]On this basis, the question of whether a State or a government can create a narrowly-tailored restriction on cyberspace anonymity without violating the privacy remains unresolved.

Anonymity often considered a cornerstone of democracy, is easier to attain than ever before, due to the recent emergence of cyberspace. Cyberspace allows people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy, free from geographic and physical constraints. Due to the nature of ICTs, identities in cyberspace are easily cloaked in anonymity. With this anonymity, cyberspace provides the means to perpetrate widespread criminal activities with little chance of apprehension.[21]

Taking a look from another perspective, anonymity in cyberspace allows whistle-blowers and political activists to express their opinions critical of employers and further the government aids and enables the entrepreneurs in acquiring and sharing technical information without alerting their competitors and permits individuals to express their views online without fear of reprisals and public hostility. It has been made clear that in various parts of the world people may have an interest in not being identified and thus connected to certain published views and opinions. Due to the international character of the Internet, those reasons for anonymous communications which are related to the "freedom of expression" may gain new dimensions.

Before the advent of the information age, a person's identity, and information relating to his or her identification has always been controlled. But all that has changed. The advent of the information society has increased the need for identifying mechanisms and thus in turn, the public availability of the relevant technologies. Names, addresses, e-mail addresses, photographs, social security numbers, etc., are freely available on the Internet and numerous

[19] George F. du, *Criminalization of True Anonymity in Cyberspace,* Michigan Telecommunications and Technology Law Review 7 1 2001

[20]Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan and SapnaTyagi, 'Cybercrime, Digital Forensics and Jurisdiction'(4th Edn. 2011 Springer) 345

[21]Supra at 19.

identity-related characteristics are for sale. The development of ICTs makes more and more people reluctant to reveal their true identity. In combination with this, different services have recently been developed which make Internet activities, such as surfing anonymous. Facilities are also anonymous. Hence, anonymous communication is promoted as the solution to the problem. However, anonymous raises various legal questions: What exactly do we mean by anonymity? Why would people want to communicate and transact on an anonymous basis? What are the practical and legal constraints upon anonymity when communicating and transacting with others? Finally, total anonymity may be possible through the use of privacy-enhancing technologies.

1.5 TYPES OF ANONYMITY

There are two different types of anonymity: true and pseudo-anonymity. However, many scholars fail to address the distinction between these types. In this article, we will distinguish between true and pseudo-anonymity, two completely different forms of expression, with differing degrees of political and social values.

- **TRUE ANONYMITY**

This kind of anonymity is not traceable. The only coincidence or purposeful self-exposure will bring the identity of the mystery sender to others; the identity of a person acting in a truly anonymous manner cannot be definitively discovered through any amount of diligence. Some attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender himself. Although a few of the forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for illegal acts because the message senders cannot be held accountable for their actions.

- **PSEUDO-ANONYMITY**

Communications are inherently traceable in pseudo- anonymity. This kind of anonymity has significant benefits; it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise. Although this allows scope for the governments to

misuse their ability to uncover the identity of people acting pseudo – anonymously, it is not in the government's interest to break that trust; by respecting pseudo-anonymous identities, governments can often avoid the far more dangerous abuses stemming from true anonymity.

1.6 SPEED

Speed has been one of the fastest evolving features of cyberspace and this speed can be understood to have two dimensions: first as an instant mode of transaction and second the expansion of the internet itself.

Speed, as an instant mode of communication, has made our life easier and faster in comparison of earlier modes of communication. The computers process data at an extremely fast speed, at millions of instructions per second. In a few seconds, a computer can perform such a huge task that a normal human being may take days or even years to complete. The unit of speed of a computer is MHz (Megahertz) i.e. one million instructions per second. At present, a powerful computer can perform billions of operations in just one second.

The other dimension of this speed is the expansion of cyberspace itself since its beginning. The Oxford dictionary defines expansion as – enlargement of scale; anything spread out; to increase in size or effect.[22]Changes in cyberspace are driven in large part by private industry research and development. The interdependency and innovation of civilian economic markets and communications industries have a direct impact on cybersecurity.

Further, the domain itself is growing and evolving as information technology and the market expands and develop. This shapes many aspects of cyberspace and drives towards a system that allows for rapid innovation.

Why does cyberspace seem to change so quickly, presenting opportunities and challenges at a greater speed than we are accustomed to in the physical world? There are a number of reasons for this change, and they are scattered throughout the twentieth century. Steady advances in technology led Gordon Moore (co-founder of Intel) to state his belief that engineers would be able to double the number of transistors on a computer chip every two years. This observation,

[22] Oxford's English Language Dictionary (18th Edn. 2018 997)

known as Moore's Law, was made in 1975 and has held true for the past four decades. It means that the speed—processing power—of computer chips increases steadily, making laptops more powerful, turning Smartphone into handheld computers, and allowing Google searches to be completed ever-faster. Squeezing more transistors onto a chip means greater speed, and speed underpins the digital world.

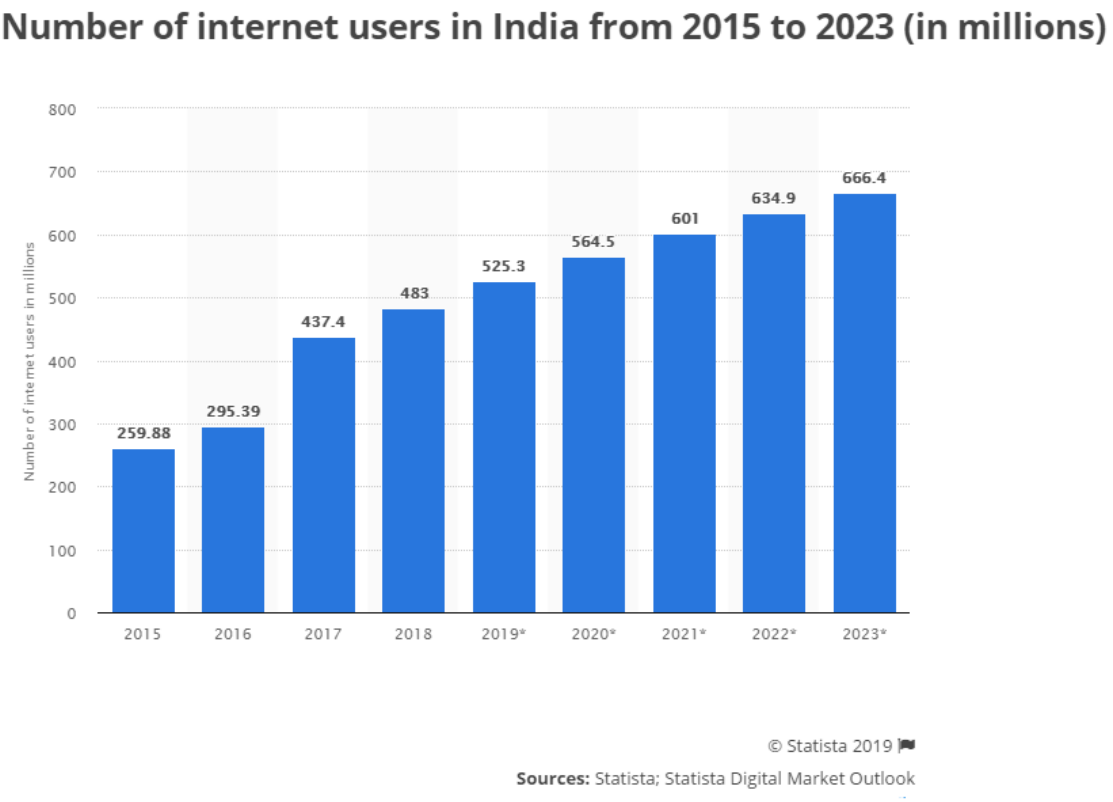
The World Wide Web was invented in the year 1989. Today there are more than 1.2 billion websites. There are 3.8 billion Internet users in 2017 (51% of the world's population of 7 billion), up from 2 billion in 2015. Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022 [23](75% of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90% of the projected world population of 8.5 billion, 6 years of age and older).

With more than 460 million internet users, India is the second-largest online market, ranked only behind China. [24]By 2021, there will be about 635.8 million internet users in India. Despite the large base of internet users in India, only 26 percent of the Indian population accessed the internet in 2015. [25]This is a significant increase in comparison to the previous years, considering the internet penetration rate in India stood at about 10 percent in 2011. Furthermore, men dominated internet usage in India with 71 percent to women's 29 percent.

This statistic provides information on the number of internet users in India from 2015 to 2023. In 2018, India had 483 million internet users. [26]This figure is projected to grow to 666.4 million internet users in 2023. Despite the untapped potential, India already is the second-largest online market worldwide. The majority of India's internet users are mobile phone internet users, who take advantage of cheap alternatives to expensive landline connections that require desktop PCs and infrastructure. As of 2016, India had 320.57 million mobile phone internet users and

[23] Steve Morgan, '*2017 Cybercrime Report'* (2018 Cyber Security Ventures) <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>
[24]Statista Research Department, Internet Usage in India- Statistics and Facts (March 31, 2020 Statista.com) <https://www.statista.com/topics/2157/internet-usage-in-india/>
[25] Ibid
[26] Supra at 24

forecasts estimate 492.68 million Indian mobile phone internet users by 2022.[27]



1.7 INTERCONNECTEDNESS

The world is moving into space where everything and everyone is connected. This technological convergence has brought about numerous changes in our day-to-day innovation for businesses. This convergence has grown stronger over time and technological dependence has increased to such a great extent that, today, we rely on some or the other form of technology for almost any aspect of our entire life. Today, business ecosystems have become an expanded universe of intelligent devices that are interconnected, indirectly or directly, via the Internet.

The Oxford dictionary defines inter as – a prefix meaning between or among and Connectivity as – the characteristic of, or suitability for, being connected, to make connections. Cyberspace comprises of interconnected physical systems that have a host of connections within the physical

[27] Supra at 24

domain. [28]The physical systems may differ in detail, but they share the common feature that they are the foundation for the next physical system connected to them. The air domain is a physical entity and airpower relies on individual systems such as platforms, bases, logistics and personnel to function as a system of systems. In contrast, the cyber domain itself is a system of systems due to the inter-connectivity of a multitude of physical systems.[29]

It is this inter-connectivity that defines cyberspace and has allowed applications like Facebook to grow to have over 700 million users in a short span of time. This aspect of the cyber domain makes it intricate, complex to define and difficult to understand. This is compounded by cross jurisdictional boundaries and attribution difficulties that provide challenging doctrinal, legal and operational implications.

Individuals as well as corporations might have ownership of some physical systems and interconnections but there is no ownership of cyberspace as a collective. This is a quality shared with the space domain noting that entry into the cyber domain is obtained at a significantly lower cost and sophistication than into space. Users of cyberspace exploit low-entry costs, widely available resources and a minimum required investment to influence the domain.

1.8 SURVEILLANCE

Global security concerns, acts of terrorism and organised crime activity have motivated nation-states to delve into implementing measures of mass surveillance in cyberspace, the breadth of which was partly revealed by the whistleblower Edward Snowden.[30]

The vast majority of computer surveillance involves the monitoring of data and traffic on the internet in the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law

[28] Oxford's English Language Dictionary (OUP 17TH Edn 898)
[29] Air Power Centre Bulletin. 'What is Cyberspace?' (Vol 157, June 2011) <https://vdocuments.mx/what-is-cyberspace-examining-its-cha-what-is-cyberspace-examining-its-characteristics.html>
[30] Theo Tryfonas, *Human Aspects of Information Security, Privacy, and Trust* (Vol. 9750, Publisher: Springer International)201-211

enforcement agencies. [31]Packet capture is the monitoring of data traffic on a computer network. Computers communicate over the Internet by breaking up messages (emails, images, videos, web pages, files, etc.) into small chunks called "packets", which are routed through a network of computers, until they reach their destination, where they are assembled back into a complete "message" again. Packet Capture Appliance intercepts these packets as they are travelling through the network, in order to examine their contents using other programs. [32]Packet capture is an information-gathering tool, but not an analysis tool. That is it gathers "messages" but it does not analyze them and figure out what they mean. Other programs are needed to perform traffic analysis and sift through intercepted data looking for important/useful information. Under the Communications Assistance For Law Enforcement Act, all U.S. telecommunications providers are required to install packet sniffing technology to allow Federal law enforcement and intelligence agencies to intercept all of their customers' broadband Internet and voice over Internet protocol (VoIP) traffic.

A large amount of data gathered from packet capturing requires surveillance software that filters and reports relevant information, such as the use of certain words or phrases, the access of certain types of web sites, or communicating via email or chat with parties. Agencies, such as the Information Awareness Office, NSA, GCHQ and the FBI, spend billions of dollars per year to develop, purchase, implement, and operate systems for interception and analysis of data. Similar systems are operated by Iranian secret police to identify and suppress dissidents. The required hardware and software was allegedly installed by German Siemens AG and Finnish Nokia.[33]

In India surveillance by the law enforcement authorities has always been an accepted practice, in fact, it was in the context of police surveillance that the two most landmark decisions on the right to privacy were pronounced by the Supreme Court. [34]Even in those two cases, one upheld the surveillance activities of the police and the other struck them down mainly on a technical ground that they were being carried on without the proper authorizations. In the modern age, however, most surveillance activities are carried on through tapping or interception of telecommunication

[31]Maddox Howe, Management of Sports and Physical Education (5thEdn EDTECH Press 2020) 351

[32]Riley Witt, Women Education in 21st Century (3rdEdn.EdTech Press 2019) 561
[33]Skylar, Vocational Education (2ndEdn.EdTech Press 2020) 91
[34] CIS India, State of Cyber Security and Surveillance in India (2018 CIS India.org) <https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf>

messages and therefore the two most important legislations in the context of surveillance today are the Indian Telegraph Act, 1885and the Information Technology Act, 2000.[35]

The Information Technology Act, 2000 ("IT Act") widely regulates the interception, monitoring, decryption and collection of information of digital communications in India. [36]More specifically, section 69 of the IT Act empowers the Central Government and the state governments to issue directions for the monitoring, interception or decryption of any information transmitted, received or stored through a computer resource. Section 69 of the I.T. Act expands the grounds upon which interception can take place as compared to the telegraph Act. [37]As such, the interception of communications under Section 69 is carried out in the interest of:

- The sovereignty or integrity of India;
- Defense of India;
- Security of the State;
- Friendly relations with foreign States;
- Public order;
- Preventing incitement to the commission of any cognizable offense relating to the above; and
- For the investigation of any offense.

It must be noted that although the grounds for interception are roughly the same as the telegraph Act (except for the condition of prevention of incitement of only cognizable offences, defense of India and the addition of investigation of any offence) the IT Act does not have the overarching condition that interception can only occur in the case of public emergency or in the interest of public safety. Additionally, section 69 of the IT Act mandates that any person or intermediary who fails to assist the specified agency with the interception, monitoring, decryption or provision

[35] National Research Council, Engaging Privacy and Information Technology in Digital Age (20th Report 2019 NRC) 567

[36] IT Act 2000

[37] IT Act 2000, s 69

of information stored in a computer resource shall be punished with imprisonment for a term which may extend to seven years and shall bailable for a fine.

1.9 LET'S SUM UP

In this chapter, we have studied the inherent characteristics of cyberspace. We have started with the concept of cyberspace, and then we have inherent characteristics of cyberspace. We have seen how these inherent characteristics are the biggest strength as well as the biggest weakness of this cyberspace. We have also discussed the impact of these features on our day to day life.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Q. 1 What are the inherent characteristics of cyberspace?

A. The inherent characteristic of cyberspace inter alia include: borderlessness, anonymous, speedy, interconnectedness, vigilant etc.

Q. 2 How is the interception and decryption of digital communication in India done?

A. The interception, decryption, monitoring and collection of digital communication is done in India as per the provisions of the Information Technology Act, 2000 enlisted under section 69 which states that interception can take place in the interest of protection of the sovereignty, defence of the country, security of the state, establishing friendly relations with neighbouring states, maintaining public order, investigating for offences, etc.

Q. 3 What are the kinds of anonymity associated with cyberspace?

A. The kinds of anonymity associated with cyberspace are true anonymity and pseudo anonymity.

Q. 4 What does the 'borderless' phenomenon of cyberspace signify?

A. Use of cyberspace defies geographical boundaries, for distance is dead in cyberspace. Hence, cyberspace is called a borderless phenomenon.

Q 5. What is the advantage of the anonymity of Cyberspace?

A. The major disadvantage of anonymity of cyberspace lies in the fact that it does not allow easy detection of the user of such cyberspace.

1.11 FURTHER READING

- https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
- https://www.statista.com/topics/2157/internet-usage-in-india/
- http://airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF157-What-is-Cyberspace-Examining-its-Characteristics.pdf
- http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1428&context=law_lawreview
- http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1380&context=californialawreview

1.12 ACTIVITY

Write an essay capturing the inherent characteristics of cyber law, thereby throwing light on the advantages and disadvantages of its usage. (800-1000 words)

Unit 3: Forms of Cyberspace Regulations

3

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Government Regulations
1.4 Self-Regulations
1.5 Technological Regulations
1.6 No Regulation
1.7 Let's sum up
1.8 Check Your Progress: Possible Answers
1.9 Further Reading
1.10 Activity

1.1 LEARNING OBJECTIVES

After studying this unit, the students should be able to understand:

- The need for regulation of cyberspace
- Aware of different modules of cyberspace regulation
- Analyze the pros and cons of each regulatory theories of cyberspace
- To know the most feasible option for cyberspace regulations.

1.2. INTRODUCTION

There have been arguments advocating that cyberspace should not be regulated and that any control in the form of regulation would stifle an unfettered potential for growth. This view arose

in response to a cumbersome web of local and national legal regimes, which added more confusion than a certainty to the cyber world. Such arguments claim that over time cyberspace will mature and so will its audience, creating a robust and socially cohesive system. These arguments, however, have little foundation.

Regulation refers to the conduct of the individual or institution to be regulated. Thus regulation encompasses three components: (1) legislation – where rules are defined, (2) enforcement – where appropriate actions are initiated against the rule violaters, and (3) adjudication – where consideration is made if the rules had indeed been breached, and where the appropriate sanctions for such breach are determined. [38]The goal of regulation is the prescription of behavioural norms. There is a great diversity of regulatory models and the norms can be divided into four categories according to their scope of application: the object, the ‘‘author, the subject and the sanction of the norm.

Regulation is necessary in Cyberspace as, without it, evidence has indicated that the cyber world will be subsumed in uncertainty and become rampant with abuse. The following example of privacy illustrates this clearly. Unregulated, cyberspace is a brutal environment, where users' rights are virtually non-existent and the remedies are confused and uncertain. An unregulated Cyberspace has the capacity to undermine entire legal systems, tear at community values and stifle commercial activity. The real purpose of this module is to stress the need for regulation of Cyberspace and the possibility and scope of its regulation.

1.3. GOVERNMENT REGULATIONS

Government regulations module is one of the prominent form of regulation where the government is regulating the affairs of cyberspace through its machinery. The legislation is one of the most significant mechanisms through which the government is regulating cyberspace worldwide. This regulation takes two forms: enforcing laws of general applicability in cyberspace and creating new laws to govern cyberspace. The adaptation of the UNCITRAL model of e-commerce for the formation of cyber laws in India is one of its examples that how Indian government framed the Information Technology Act 2000. This act also amended existing

[38]R Y COng, 'Mobile Communication and Protection of Children' (Leiden University Press 2011) 45

laws such as the Indian Penal Code, 1860, Indian Evidence Act, 1872, Bankers Book of Evidence etc. this legislation addressed various legal concerns such as legal recognition of electronic documents, recognition of electronic authentication mechanism, jurisdictional concerns of cyberspace and regulation of cyber offence and cyber contraventions. Sometimes court intervention becomes essential to regulate the affairs of cyberspace as well as deficiencies of cyberspace. The best illustration of judicial intervention can be found in the case of ***ShreyaSinghalvs Union of India***[39] which held '***section 66 A unconstitutional because it violates freedom of speech and expression in cyberspace which is one of the fundamental right enshrined under Indian constitution'.***

Although still there are some grey areas in this regulatory module. In cyberspace, distance is measured in nanoseconds - not miles. Social interaction or commercial transactions on a transnational level are possible with ease here to fore only imagined by science fiction writers who dreamed of teleportation devices. Accordingly, one is as likely to have an international dispute as a national one. The function of dynamic routing and facilities such as the World Wide Web, File Transfer Protocol, and remote log-on/telnet permit a user to enter, or at least to cross numerous national, state, or local borders without either the user or national authorities being aware of the user's passage. Therefore, "traditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces but networks, domains, and hosts."[40]

Trying to regulate cyberspace on a country-by-country basis is doomed to fail because it is inefficient and does not account for the inherent nature of the technology. "The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location." [41]"The unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes." Similarly, the unique nature of the cyberspace requires a uniform global system of regulation should bar nation-states from enacting inconsistent national legislation. Apart from these concerns, excessive internet censorship is one of the biggest criticisms of

[39]*ShreyaSinghal v Union of India*[2013] 12 S C C 73
[40]Anup K Ghosh, E-commerce Security and Privacy (1ST Edn. Spinger-Business Media LLC 2001) 91
[41]Communications Policy and Information Technology: Promises, Problems, Prospects, Communication Research Conference on Information, and Internet Policy (29th : 2001 : Washington D. C.)

government regulation. The Great Digital Firewall of China is one the best illustration to site on this issue.

1.4. SELF-REGULATIONS

Self-government or self-regulation is usually justified if it is: (1) more efficient; (2) the rules or adjudicatory procedures differ from the surrounding community; (3) the rules of the surrounding community are inapplicable; or (4) compliance with the rules of the community is higher, if the rules are self-enforced. Although all four factors support self-regulation, this section will focus on the first. The jurisdictional and sovereignty issue in cyberspace makes it difficult for territory-based nation-states to enforce their laws on cyberspace. Even if jurisdictional issues are solved, the infrastructure of cyberspace is evolving too rapidly for governments to regulate efficiently. The unique technical and transnational nature of cyberspace justifies self-government.

Users of the Internet rely on 'netiquette', the day to day rules for dealing with others on the Internet. They are in effect a form of customary law. The culture is widely prevalent, though the rules vary in their details. [42]If necessary they are enforced by non-legal remedies, which John Perry Barlow, the founder of the Electronic Frontier Foundation in the US, describes as ***'self-regulation'***. The technology itself allows these norms to be reinforced by users. The basic idea of self-regulation is that a community can police itself through either the development of norms of conduct, private law enforced by contract, technological architecture, or some combination of the three.

P. Trudel (1989) defines this concept as norms voluntarily developed and accepted by those who take part in an activity. Self-regulation encompasses a large number of concepts such as codes of conduct, model contracts, codes of ethics, memorandum of understanding, technical or administrative standards, certification or labelling systems. The technology itself may equally have a normative effect on behaviour and might become a source of the Internet Law when the parties are contractually referring to it or when an authority imposes it as a ***de jure (or de***

[42]Helen Robert, 'Can the Internet be Regulated?' (AUP.GOV 2011 22) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/RP9596/96rp35>

facto)technical standard. This self-regulation, including the standard-setting process, affects fundamental public concerns and are no longer technical rules of purely commercial interest

Overall, the legislatures, regulatory agencies, and courts do not appear to be percipient in anticipating the economic and social impact of new technology. This lack of foresight suggests that these institutions should not ***unnecessarily***exercise their existing authority and not seek new authority to regulate cyberspace until either the technology and its implications become predictable or the institutions and customs of cyberspace have an opportunity to develop in response to the needs of Cyberian constituent communities and commerce. Accordingly, governments should encourage a self-regulation model.

1.5. TECHNOLOGICAL REGULATIONS

Regulators can choose whether to regulate with rules or standards. A regulator may use a standard, and thus give greater discretion to the enforcement authority, or a regulator may choose to use a rule to specify the particular outcome. Technological regulations have more in common with legal rules and do not fit neatly into the category of standards. Like rules, they regulate user behaviour, in contrast to technical standards, which merely regulate form.

In network environments, the term "standard" is largely understood to mean uniform physical and design specifications or metrics.' Like its predecessor, the legal standard, the technical standard regulates form. The infrastructure of cyberspace, for example, is defined by a unified architectural structure and standardized protocols, collectively known as the formal TCP/IP networking reference model. Technical standards do not raise serious normative issues, because they are concerned only with the form and value measurements of the Internet's infrastructure, such as quality assurances, bit size, and attached transit services.

With the evolution of standard-setting from technical to "technological" standards, that truth is no longer categorical. While technical standards regulate form, technological standards more directly regulate user behaviour. Such technological standards embed normative choices set by program designers. When technological products are standardized, firms may manipulate such standards for competitive or other advantages." Thus, technological standards, like other

delineated legal entitlements of property, may overprotect the creation and recognition of property rights in intellectual goods.

Technological designs, such as digital rights management (DRM), can be understood as a form of policymaking that may supplement or even supplant legal rules governing behaviour. Once constraints on behaviour are built into technology, the technological standards established by the constraints effectively govern the use of that technology in a manner that competes with law. Technological standards may be seen as equivalent to a licensing regime or as a form of copyright law. In some cases, technological standards can be more anticompetitive than legal rules and may give rise to antitrust concerns. From an institutional standpoint, the legal challenges created by standardized technology are present not only when firms standardize technology themselves but also when governments do so.Because technological standards act as law, they should be subjected to an optimal lawmaking analysis.

An example of a technologically designed legal command that regulates user behaviour is the standardized serial copy management system, which permits record companies to control digital copying of recorded music. In essence, it supports standardized digital equipment containing legally mandated features.

FORM REGULATION: TECHNICAL STANDARDS

When legal commands that regulate form are promoted through legal rules, they are characterized by a high level of specificity backed by an authoritative executing mechanism that leaves little room for judicial discretion. Such are many of the rules regulating civil and criminal procedural law. When commands are designed as legal standards, they are typically characterized by the level of the technical value measurements such as the quantity, weight, extent or quality they provide.

In network environments, such as cyberspace, the term "technical standards" generally means uniform physical and design specifications or metrics and, as such, technical standards are regulations of form. Formal technical standards have evolved through three categories that together define the scope of technical standards: "representational standards," "unit standards," and "similarity standards". Representational standards, the most basic class of technical

standards, define abstract quantities. Examples of representational standards are the number system, addresses, currency, and mathematical notation, such as +, -, and %. They are arbitrary human constructs without a corresponding physical representation. Unit standards define physical quantities, such as meters, miles, grams, volts, and seconds. Occasionally, these two categories of standards are combined. Human language is such a case, as it is based on specific sounds made by the human voice. In network environments, unit standards include the Open System Interconnect (OSI) reference model of the Internet's architecture, and the American Standard Code for Information Interchange (ASCII) character set, the most common standard for the 128 code numbers used by computers to represent all upper- and lowercase Latin letters, numbers, and punctuation. Lastly, similarity standards are groupings of a specific unit and representational standards that define the common physical properties of two or more entities, usually to provide some interchangeability in manufacturing, distribution, sales, and use.

In network environments, many communication standards, especially protocol standards, behave like similarity standards. ‘They define transmitting and receiving pairs, process definitions, and even quality test procedures. An example of a similarity standard in a network environment is the industry standard for information systems, the Internet ISO/IEC 15288 "Life Cycle Management-System Life Cycle Processes." **ISO/IEC** 15288 establishes a common cyclical production process of system technologies, such as the Internet, describing their technical value measurements and associated terminology.

Standards that regulate formal value measurement specifications are not unique to cyberspace. They existed in earlier information technology industries, particularly mobile telephony, high definition television (HDTV), and the radio frequency spectrum. Ultimately, the correlation between standards and form regulation was imported into the emerging governance of cyberspace. Primarily, the Department of Commerce limited the authority of the Internet Corporation for Assigned Names and Numbers (ICANN), which controls the Internet's domain name system, to "technical coordination" or routine "maintenance. In that limited regulative capacity, ICANN controls technical issues such as the maintenance of the bit size of data packets, the architecture of root services (which involves assigning Internet protocol (IP) numbers and specifying the number of top-level domains that safely be added to the root), and the preservation of unique protocol numbers for various other Internet functions. Thus, the U.S.

government authorized ICANN solely to construct technical standards aimed at regulating form but did not give ICANN any authority to regulate user behaviour. Nevertheless, this policy is not fully exhaustive or consistent, though, as both types of standards seem to be loosely merged in the 1997 Report.

SUBSTANCE REGULATION: BEHAVIORAL TECHNOLOGICAL STANDARDS

In the information age, technical standards have increasingly been incorporated into operational software designs that influence user behavior. Ultimately, the design process of these standards started to resemble the design process of software programs containing mandatory legal commands. Thus, technological standards became an aspect of software design and standard developers became closely related to programmers. To illustrate, when a specific software program is used as a testbed, the specific program in the testbed takes on the characteristics of a technological standard, implementing the information it contains. This shift is particularly evident with the development of DRM. As new markets and submarkets in network environments expand, businesses are experimenting with distribution models, such as dynamic pricing, permission to view content in exchange for user demographics, and syndication of content to other websites. One of the most controversial of these developments is DRM technology developed **by** copyright-driven industries. DRM software prevents purchasers and third parties from making unauthorized uses of digital works.**DRM** technology has two separate functions. First, it identifies digital versions of copyrighted works, just as international standard book numbers (ISBN) identify hardcopy books and stock-keeping unit (SKU) numbers identify retail merchandise." Copyright owners use two main types of existing technologies, known as "watermarking" and "fingerprinting, to create digital identifications for their works. The identification function tracks works electronically, such as when they are transmitted over basic peer-to-peer networks in the form of email or instant message attachments.

Second, DRM software may also provide copyright owners with control over the various excludable rights of copyright ownership, including access to their works and the ability to make copies of and redistribute the works. At the heart of any DRM technology is the business notion of a rights model: a scheme for stipulating to users rights to a portion of content in return for a consideration, such as registration, payment, or consent to the tracking of his or her usage.

Alternatively, many networks have architectural designs and technological standards that implement the norm of open information access.

There are two new types of technological standards specific to network environments: "compatibility standards" and "adaptive standards." Compatibility standards specify a grouping of similarity standards to support local or remote communications between independent implementations. Adaptive standards are open-ended, and allow the specification of areas left open for future revisions, manufacturer-specific options, and further study. They specify a negotiation process concerning the exchange of data between separate technological systems that includes two or more compatibility standards, and are used to establish communications.' The ability of users to access USENET, FTP, or WWW on the Internet is such a form of negotiation. Examples of adaptive standards are the IETF Internet draft 11 and the protocol extension protocol, which are designed to accommodate extensions of applications such as hypertext transfer protocol (HTTP) clients, servers and proxies. Adaptive standards allow each compatibility standard to negotiate a range of variables, including quality of communication, quantity of data transmitted, and other parameters of these systems. Thus, when protocols are open-ended by design and are used for negotiation instead of nonnegotiable incompatible transfer of user data and control, they may be considered adaptive standards. Because of the widespread use of programmable processors and the similarity to sophisticated software programs, adaptive standards are becoming increasingly important both technologically and as a mechanism to regulate user behavior.

Technological standards, which directly regulate behavior, are a different category of standards than technical standards, which only regulate form. In terms of optimal lawmaking analysis, technological standards are closely related to legal rules. For example, both substantive rules and technological standards influence user behavior directly. As technological standards' influence on behavior increases, they will increase in similarity to legal rules. Rules are best promulgated by centralized institutions, particularly public, governmental institutions. In network environments such as the Internet, however, centralized regulation is unable to keep pace with the dynamic commercialized nature of technology. Thus, the technique commonly known as technological standardization is still best kept decentralized.

1.6 NO REGULATION

The no regulation model is a null choice because, in cyberspace, the idyllic state of nature never actually existed. Cyberspace is an accidental byproduct of United States government research. Consequently, the United States government has always placed some regulation on cyberspace. For example, the NSFNET Backbone Services Acceptable Use Policy prohibits the commercial use of NSFNET. At all times the physical bodies of Cyberians could be punished for their cyberspace activities should some "real" government choose to exercise such control. Yet, governments rarely attempted to extend their jurisdiction into cyberspace. But this policy of benign neglect has changed. Governments are now interested because many individuals who are currently using the Internet can afford to invoke the judicial system to resolve disputes. The popularization of the information superhighway has educated both judges and legislatures that this is a place where real wrongs take place - wrongs that are worthy of a remedy.

1.7. LET'S SUM UP

In this chapter, we have studied the concept of cyberspace regulations. We have started with the concept of regulation of cyberspace. Then we have learnt different modules of cyberspace regulation. We have seen how these modules regulating the affairs of cyberspace. We witnessed none of the regulatory theory in isolation is completely able to regulate the cyberspace. Every theory having some pros and cons with respect to their ability in regulating cyberspace.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the necessary ingredients of regulations that address cyber laws and cyberspace?

A. The necessary ingredients of regulations that address cyber laws and cyberspace include i) legislation, ii) enforcement and iii) adjudication.

2. How has the government addressed the regulations associated with cyberspace?

A. The government addressed the regulations associated with cyberspace primarily by adapting the UNCITRAL model of e-commerce for establishing cyber laws in the country, and thereby paving the way for introduction of cyber laws in existing statutes like Information Technology Act, 2000, Indian Penal Code, 1860, Indian Evidence Act, 1872, Bankers Book of Evidence Act, etc.

3. What does cyberspace regulation aim at?

A. The aim of cyberspace regulation is to define the rules associated with use and implementation of cyberspace, to initiate appropriate actions against those who violate such regulations and adjudicating the extent of breach of such violations and imposing the required sanctions.

4. What are the positive aspects of self-regulations?

A. The positive aspects of self-regulations are that they are efficient, the rules and adjudicatory procedures differ from the surrounding community whereby the latter become inapplicable and compliance with the rules of the community is higher.

5. What is understood by DRM?

A. DRM or Digital Rights Management is a form of technological design that can be understood to be a form of policy making that may supplement or even supplant legal rules governing behavior.

1.9 FURTHER READING

- Daniel Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 Cal. L. Rev. 1069 (2004). Available at: http://scholarship.law.berkeley.edu/californialawreview/vol92/iss4/5
- https://repository.jmls.edu/cgi/viewcontent.cgi?article=1055&context=jitpl

- Jangirala, Srinivas& Das, Ashok Kumar & Kumar, Neeraj. (2018). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems. 92. 10.1016/j.future.2018.09.063.

1.10 ACTIVITY

Elucidate the forms of regulations along with a case study that briefly explains the regulation theories of cyberspace? (1500-2000 words)

Unit 4: Cyberspace Regulatory Theory of Lawrence Lessig

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Law as a means of Regulation

1.4 Role of Market force in Regulation

1.5 Norms as Regulatory Mechanism

1.6 Code or Architecture in Cyberspace Regulation

1.7 Let's sum up

1.8 Check Your Progress: Possible Answers

1.9 Further Reading

1.10 Activity

1.1 LEARNING OBJECTIVES

After studying this unit, the students should be able to understand:

- Define the pathetic dot theory
- Aware of different constraints pathetic dot theory viz. law, norm, market and codes.
- Interrelationship amongst these four constrains in cyberspace regulation. internet

1.2. INTRODUCTION

There are many ways to think about "regulation." Lawrence Lessig thinks about it from the perspective of someone who is regulated, or, what is different, constrained. That someone

regulated is represented by this (pathetic) dot—a creature (you or me) subject to different regulations that might have the effect of constraining the dot's behaviour. By describing the various constraints that might bear on this individual, Lessig attempted to show how these constraints function together. This idea of regulation by Lessig is known as the Pathetic Dot Theory.

Lawrence Lessig explained the regulation and the role of these four constraints with the illustration of smoking. [43]If one wants to smoke, what constraints does one face? What factors regulate the decision to smoke or not? One constraint is legal. In some places at least, laws regulate smoking—if you are under eighteen, the law says that cigarettes cannot be sold to you. If you are under twenty-six, cigarettes cannot be sold to you unless the seller checks your ID. Laws also regulate where smoking is permitted—not allowed on an airplane, or in an elevator, for instance. In these two ways at least, laws aim to direct smoking behavior. They operate as a kind of constraint on an individual who wants to smoke. But laws are not the most significant constraints on smoking. Although this illustration is not efficiently depicting the situation in India because of stringent and effective implementation of smoking laws.

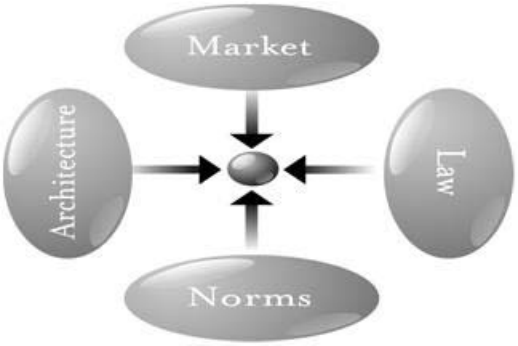
He tried to explain how by norms smoking can be regulated. Norms say that one doesn't light a cigarette in a private car without first asking permission of the other passengers. They also say, however, that one needn't ask permission to smoke at a picnic. Norms say that others can ask you to stop smoking at a restaurant, or that you never smoke during a meal. These norms affect a certain constraint, and this constraint regulates smoking behavior.

Laws and norms are still not the only forces regulating smoking behavior. The market is also a constraint. The price of cigarettes is a constraint on your ability to smoke—change the price, and you change this constraint. Likewise with quality. If the market supplies a variety of cigarettes of widely varying quality and price, your ability to select the kind of cigarette you want increases; increasing choice here reduces constraint. Finally, there are the constraints created by the technology of cigarettes, or by the technologies affecting their supply. Nicotine-treated cigarettes are addictive and therefore create a greater constraint on smoking than untreated cigarettes. Smokeless cigarettes present less of a constraint because they can be smoked in more places. Cigarettes with a strong odor present more of a constraint because they can be smoked in fewer

[43]Lawrence Lessig, Code 2.0 (Basic Books New York 3rd Edn. 2006) 54

places. How the cigarette is, how it is designed, how it is built—in a word, its architecture—affects the constraints faced by a smoker.

Thus, four constraints regulate this pathetic dot—the law, social norms, the market, and architecture—and the "regulation" of this dot is the sum of these four constraints. Changes in any one will affect the regulation of the whole. Some constraints will support others; some may undermine others. Thus, "changes in technology may usher in changes in . . . norms," and the other way around. A complete view, therefore, must consider these four modalities together.



Above said picture explained that how these four constraints can regulate any entity. In this drawing, each oval represents one kind of constraint operating on our pathetic dot in the centre. Each constraint imposes a different kind of cost on the dot for engaging in the relevant behavior—in this case, smoking. The cost from norms is different from the market cost, which is different from the cost from law and the cost from the (cancerous) architecture of cigarettes.

The constraints are different, yet they are plainly mutually supporting. Each can support or oppose others. Technologies can weaken norms and laws; they can also support them. Some constraints make others possible; others make some impossible. Constraints work together, though they function differently and the effect of each is distinct. Norms constrain through the stigma that a community imposes; markets constrain through the price that they exact; architectures constrain through the physical burdens they impose; and law constrains through the punishment it threatens.

We can call each constraint a ***"regulator"***, and we can think of each as a distinct modality of regulation. Each modality has a complex nature, and the interaction among these four is also hard to describe. I've worked through this complexity more completely in the appendix. But for

now, it is enough to see that they are linked and that, in a sense, they combine to produce the regulation to which our pathetic dot is subject in any given area. We can use the same model to describe the regulation of behavior in cyberspace.

Now we will discuss of these four constraints regulates the affairs of any entity in cyberspace.

1.3. LAW AS A MEANS OF REGULATION

Behavior in the real world — this world, the world in which I am now speaking — is regulated by four sorts of constraints. Law is just one of those four constraints. Law regulates by sanctions imposed ex-post — fail to pay your taxes, and you are likely to go to jail; steal my car, and you are also likely to go to jail. Law is prominent of regulators. But it is just one of four.

We believe in parliament's capacity to make laws to regulate the behaviour of its citizens. Where parliaments are silent, the courts will make precedents. People who break the law suffer sanctions - these can be civil penalties of loss of money when an infringing party is ordered to pay damages to another. There is also criminal law through which we believe society establishes what constitutes acceptable and unacceptable behaviour. Unacceptable behaviour is regulated through a sentencing regime – lesser offences might incur fines and bonds, more serious ones some form of a custodial sentence. We are satisfied that if parliament makes a law then it is made by the people. What is the parliament if nothing other than a delegate body of the people as articulated at elections? Once a matter becomes law the law itself ought to be a black letter – it ought to be clearly understood, free from doubt and dispute. Breaches should result in similar punishments.

Law regulates behavior in cyberspace. Copyright law, defamation law, and obscenity laws all continue to threaten ex post-sanction for the violation of legal rights. [44]How well law regulates, or how efficiently, is a different question: In some cases, it does so more efficiently, in some cases less. But whether better or not, the law continues to threaten a certain consequence if it is defied. Legislatures enact; prosecutors threaten; courts convict. We can take an illustration of Indian cyber laws that how it is regulating affairs of entities of cyberspace through framing various new legislations and by amending existing legislation.

[44]David Brake, Sharing our Lives Online: Risks and Exposure in Social Media (Palgrave Macmillan 2014) 78

Law can also regulate other constraints such as the market. The market is regulated by law not just in its elements—it is the law that enforces contracts, establishes property, and regulates currency—but also in its effects. The law uses taxes to increase the market's constraint on certain behaviors and subsidies to reduce its constraint on others. We tax cigarettes in part to reduce their consumption, but we subsidize tobacco production to increase its supply.[45] We tax alcohol to reduce its consumption. We subsidize childcare to reduce the constraint the market puts on raising children. In many such ways, the constraint of law is used to change the constraints of the market.

Law can also change the regulation of architecture. Lessig explained it as follows:

Some of the power of the French Revolution derived from the architecture of Paris The city's small and winding streets were easily barricaded, making it possible for revolutionaries to take control of the entire city with comparatively little absolute strength. Louis Napoleon III understood this, and in 1853 he took steps to change it. Paris was rebuilt, with wide boulevards and multiple passages, making it impossible for insurgents to take control of the city.

Likewise, law can regulate the architecture of cyberspace by making specific laws for intermediaries and by changing data protection mechanism.

Law can change social norms as well, though much of our constitutional jurisprudence seems dedicated to forgetting just how. Education is the most obvious example. As Thurgood Marshall put it, ***"Education is not the teaching of the three R's. Education is the teaching of the overall citizenship, to learn to live together with fellow citizens, and above all to learn to obey the law."***[46] Education is, in part at least, a process through which we indoctrinate children into certain norms of behavior—we teach them how to "say no" to sex and drugs. We try to build within them a sense of what is correct. This sense then regulates them to the law's end. Thus we have seen that how law as a separate constraint having an impact on rest of three constraints.

1.4. ROLE OF MARKET FORCE IN REGULATION

The market is the third constraint. It regulates by price. The market limits the amount that I can spend on clothes; or the amount I can make from public speeches; it says I can command less for

[45] Supra at 43

[46] Charles LZeldon, Thurgood Marshall: Race, Rights, and the Struggle for a More Perfect Union (Routledge 2013) 23

my writing than Madonna, or less from my singing than Pavarotti. Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates.
Markets regulate behavior in cyberspace. Pricing structures constrain access, and if they do not, busy signals do. (AOL learned this quite dramatically when it shifted from an hourly to a flat-rate pricing plan.) Areas of the Web are beginning to charge for access, as online services have for some time. Advertisers reward popular sites; online services drop low-population forums. [47]These behaviors are all a function of market constraints and market opportunity. They are all, in this sense, regulations of the market.[48]

We are convinced that market forces regulate behaviour. If a manufacturer creates an unsafe product this will become known to the market and consumers will not purchase these products. If a software designer wants to copyright and licence his or her work, then the market will determine if the software is worth buying as compared with that of competitors. Markets will determine what survives and what doesn't in the market place. Market forces also use price as a form of regulation. It is said consumers regulate their behavior based on a cost/benefit analysis. For example, at least theoretically, as the price of petrol rises, consumers will travel less in their cars and take public transport, or push for its installation. In its purest form, you believe that free markets, rather than the government, will best regulate human activity. In the case of cyberspace this can be understood how the accessibility of the internet very much depends on the and price charged for the accessibility of internet. It can be understood by Jio plan for accessibility of the internet and how it increases the accessibility of the internet in India.

1.5. NORMS AS REGULATORY MECHANISM

Social norms are a second. They also regulate. Social norms — understandings or expectations about how I ought to behave, enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community — direct and constrain my behavior in a far wider array of contexts than any law.[49] Norms say what clothes I will wear — a suit, not a dress; they tell you to sit quietly, and politely,

[47] Supra at 44
[48]Raymond S R Ku, Cyberspace: Cases and Materials (4thEdn. WoltersKuwer 2016) 67
[49]Richard A Spinello, Herman TTavani , Readings in Cyberethics (Jones and Barlett Publishes 2ndEdn 2004) 341

for at least 40 minutes while I speak; they organize how we will interact after this talk is over. Norms guide behavior; in this sense, they function as a second regulatory constraint. [50]

1.6 CODE OR ARCHITECTURE IN CYBERSPACE REGULATION

And finally, there is the constraint of what some might call nature, but which I want to call "architecture." This is the constraint of the world as I find it, even if this world as I find it is a world that others have made. That I cannot see through that wall is a constraint on my ability to know what is happening on the other side of the room. That there is no access-ramp to a library constrains the access of one bound to a wheelchair. These constraints, in the sense I mean here, regulate.David Hackett Fisher describes the founders of New England meticulously laying out the towns they would found so that the relationship of the buildings to each other, and to the town square, would assure that behavior within the town would be properly regulated.

In this constraint, we believe in the power of human to design systems that regulate behavior. To control speeding in a back street we would design and build speed humps. In a digital world, we believe in the power of software code to be able to create a form of regulation. For example, we might design a technological protection measure in our software that prevents a program with a license of ten users from allowing an eleventh user to open it over a network.

Bentham famously described the design of a prison so that all cells would be viewable from one central position so that prisoners would never know whether they were being watched, but that they always could be being watched, and so, they would be properly regulated.
An analogue for architecture regulates behavior in cyberspace— code. The software and hardware that make cyberspace what it constitutes a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace. In some places (online services such as AOL, for instance) you must enter a password before you gain access; in other places, you can enter whether identified or not. In some places the transactions you engage in produce traces that link the transactions (the "mouse droppings") back to you; in other places, this link is achieved only if you want it to be. In some

[50] Ibid

places you can choose to speak a language that only the recipient can hear (through encryption); in other places encryption is not an option. [51]The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it is also regulation, just as the architectures of real-space codes are regulations.[52]

1.7. LET'S SUM UP

In this chapter, we have studied the Lawrence Lessig approach of regulation in his pathetic dot theory. We have learnt different constraints of cyberspace regulation viz. law, market, norm and code as described by Lessig in his theory. We have also understood that how these four constraints interrelated to each other and having an impact on each other's role in cyberspace. As per the approach of Lessig he considers 'code is law'. He thinks it is code which can effectively regulate the entities of cyberspace in comparison to other constrains. Although there are some serious criticism of his view but still his view still seems relevant while thinking about regulation of cyberspace. Finally, we can end the discussion of cyberspace regulation that in isolation none of the constraint can aptly regulate the entities of cyberspace, we need to consider the interrelation of each other while developing any framework for cyberspace regulation.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. How did Lessig explain the role of the constraints vis-à-vis regulation?

A. Lessig explained the role of the constraints vis-à-vis regulation through the illustration of smoking and the constraints associated therewith, for example legal. He explained that norms can regulate certain behavior thereby acting as a constraint in its exercise.

[51] William Magnuson, Blockchain Democracy: Technology, Law and the Rule of the Crowd (Cambridge University Press 2020) 567

[52]Roger Brownsword, Eloise Scotford, Karen Yeung, The Oxford Handbook of Law, Regulation and Technology (Oxford University Press 2017 1st Edn) 89

2. What are the four basic limbs of Lessig's constraint theory?

A. The four basic limbs of Lessig's constraint theory are law, social norms, market and architecture.

3. What kind of laws regulate behavior in cyberspace?

A. Behaviour in cyberspace is regulated through laws like defamation law, copyright law, obscenity laws, regulation of the market through enforcement of contracts, the establishment of property, regulation of currency etc.

4. How can market forces regulate behavior in cyberspace?

A. Market forces regulate pricing structures which in turn affect market access so as to affect consumers' approach towards certain products and hence affecting behavior in cyberspace.

1.9 FURTHER READING

- http://pne.people.si.umich.edu/kellogg/045.html
- https://harvardmagazine.com/2000/01/code-is-law-html
- https://www.kcoyle.net/lessig.html
- https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1422&context=facpubs
- Understanding Lessig: implications for European Union cyberspace policy, Taylor & Francis (2019), https://www.tandfonline.com/doi/abs/10.1080/13600860500348226?mobileUi=0&journalCode=cirl20 (last visited Nov 18, 2019).

1.10 ACTIVITY

Write an essay on the critical analysis of Lessig's theory of regulation of cyberspace. (800-1000 words)

Block 2

Fundamentals of Cyber Law

Unit 1:Outline of Legislative Framework for Cyber Law

1

SUBJECT CODE: 101

CYBERSPACE AND ITS GOVERNANCE

BLOCK 2 – FUNDAMENTALS OF CYBER LAW

UNIT 1 – OUTLINE OF LEGISLATIVE FRAMEWORK FOR CYBER LAW

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Need for cyber law

1.4 Concept of cyber law

1.5 Jurisprudence of cyber law

1.6 Important terms related to cyber law

1.7 Interdisciplinary laws within cyber law

1.8 International Framework of cyber law

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Need and Concept of cyber law
- Jurisprudence of cyber law
- Legislative framework of cyber law

1.2 INTRODUCTION

The tremendous growth and development of electronic commerce over the last decade has propelled the need for vigorous and effective regulatory mechanisms which would strengthen the legal infrastructure. All these mechanisms and infrastructures come under the purview of Cyber Law. Cyber Law has been described as that branch of law which deals with legal issues pertaining to the use of inter-networked information technology. The virtual world of internet such as computers, networks, data storage devices etc. is known as Cyberspace and the laws governing these areas are called Cyber Laws.

Cyber Law is important as it encompasses all aspects of transactions and activities on and involving the cyberspace. Cyber Law comprises of laws relating to –

- Cyber crimes
- Electronic and Digital Signatures
- Intellectual Property Rights
- Data Protection and Privacy

In India, Cyber Laws are contained in the Information Technology Act, 2000 (IT Act) which was introduced on October 17, 2000.[53] The primary purpose of the Act is to administer legal recognition to electronic commerce and to expedite filing of electronic records with the Government.

The following Act, Rules and Regulations are enclosed under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

1.3 NEED FOR CYBER LAW

[53] Ajay Thakur, 'All You Need To Know About Cyber Laws In India - Ipleaders' (*iPleaders*, 2020) <https://blog.ipleaders.in/need-know-cyber-laws-india/>

Digitalization has transmuted the society as a whole. The advancement of technology and intertwined connections have paved way for a plethora of cybercrimes being committed at an unprecedented level.[54] Prior to this amelioration, the Internet was used and developed for sharing research and information in an unregulated manner. At present, it has become more transactional with enormous amount of data being transmitted via e-commerce, e-procurement, e-governance etc. Every person with a digital footprint has the power and capability to inflict considerable damage and cause calamitous harm to individuals, companies, and governments by accessing any data across the globe. Owing to such extensive development in informational technology, the word 'Privacy' has been completely taken off the books. In the light of the prodigious growth in digital population where people have become more sophisticated in the use of technology, data privacy and data protection have become the need of the hour. A robust regime has to be formulated that would deliver a careful and sensitive balance between the interests of the individual and legitimate concerns of the state.[55] All these and other varied considerations instigated a conducive atmosphere for the need for enacting pertinent cyber laws in India.

1.4 CONCEPT OF CYBER LAW

Cyberlaw is a generic term which refers to all legal and regulatory aspects of Internet and the World Wide Web.[56] Anything emanating from any legal issues concerned with any activity of citizens and others in Cyberspace comes within the ambit of Cyber Law. "Cyber" is a prefix word used to describe a person, thing or idea connected with computer, internet and information era. It has been taken from 'Kubernētēs', a Greek word for '*steersman'* or *'governor'*. The word *'Cyber'* was first used in '*Cybernetics'*, coined by Mr. Norbert Wiener, which means, a study of communication and control systems in living beings and machines.[57] A vast array of information resources and services on the Internet not only provides great facilities to the society but also present opportunities for crime. The very concept of the Internet lost its essence years ago when

[54]AdemolaAdeniyi, the Need for Data Protection Law in Nigeria httpas://adeadeniyi.wordpress.com accessed on 28/10/2015

[55] Trout, B (2007) "Cyber Law: A Legal Arsenal For Online Business", New York: World Audience, Inc

[56]'CYBERLAW : PERBANDINGAN INDONESIA , SINGAPURA, DAN JEPANG' (*AndreSeptian*, 2020) <https://andreserr.wordpress.com/2015/06/10/cyberlaw-perbandingan-indonesia-singapura-dan-jepang/>

[57]Poltenson, Norman. "Mohawk Valley Is the Epicenter in the Cybersecurity Industry." The Business Journal - Central New York, vol. 30, no. 21, Central New York Business Journal, May 2016, p. S9

it got transformed for being used in several illicit and immoral activities. Several unlawful activities have been taking place acorss cyberspace, ranging from identity theft and terrorism to money laundering. Taking advantage of the anonymity offered by the internet, anybody can indulge in any sort of criminal activities with impunity. Credit card frauds, spams, defamation on the social networking sites and piracies are some of the disadvantages resulting from the illegal activities on the internet.[58] These 'grey areas' are being exploited by individuals, companies to perpetrate criminal activities in cyberspace. Cyber Law has emerged to put an embargo due to proliferation of misuse of the computer and internet in the cyberspace.

1.5 JURISPRUDENCE OF CYBER LAW

Jurisprudence has been defined as *'knowledge of law or knowledge of just and unjust'*. The two Latin words 'jus' and 'prudentia' are mutated as jurisprudence in english. Legal issues relating to digital platforms and the internet in this contemporary world have brought cyber jurisprudence into existence. Cyber Jurisprudence gives an analysis of the law regardless of territorial limitations in a space completely different from the physical world.[59] It deals with the composite idea of cyber jurisdiction and cyber court's venue in cyberspace. It provides emphasis on observing cyber uniform rules and policies at an international level. In the context of Cyberspace, Jurisprudence is manifestation of its progression and collective regulatory processes to curb all the unlawful and illicit activities through enforce laws. Cyberspace has reached an inconceivable level wherein there are no jurisdictional boundaries. For instance, an individual in India could break into the electronic vault of a bank situated in the USA using a laptop or a computer or a cellphone. Cyber Legal Jurisprudence should be an evolving process and be on the same page with the technological advancement and severity of consequential effects of

[58]'CYBERLAW : PERBANDINGAN INDONESIA , SINGAPURA, DAN JEPANG' (*AndreSeptian*, 2020) <https://andreserr.wordpress.com/2015/06/10/cyberlaw-perbandingan-indonesia-singapura-dan-jepang/>
[59]'Term Paper On Cyber Jurisprudence - Assignment Point' (*Assignment Point*, 2020) <https://www.assignmentpoint.com/science/computer/term-paper-on-cyber-jurisprudence.html.>

cybercrimes. The penalties and punishments need to have a reformative or deterrent effect on the ones committing such crimes based on the seriousness of the criminal act.[60]

In India, two legislations were passed by the Indian Judicial system to deal with cyber offences in the country i.e., The Information Technology Act, 2000 and The Information Technology (Amendment) Act, 2008. The provisions of both the laws prosecute those offences committed using computer as a medium and tool. The act penalizes various cybercrimes and provides strict punishments (imprisonment terms up to 10 years and compensation up to 1 crore rupees).

1.6 IMPORTANT TERMS RELATED TO CYBER LAW

"Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary. (Section 2(1) (b) of IT Act, 2000)[61]

"Certifying Authority" means a person who has been granted a license to issue an electronic signature certificate under section 24. (Section 2(1) (g) of IT Act, 2000)[62]

"Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing electronic signature certificates. (Section 2(1) (h) of the IT Act, 2000)

"Communication Device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or images. (Section 2(1) (ha) of the IT Act, 2000)

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. (Section 2(1) (i) of the IT Act, 2000)

[60] Emerging Technologies and the Law: Forms and Analysis, by Richard Raysman, Peter Brown, Jeffrey D Neuburger and William E Bandon, III. Law Journal Press, 2002-2008 ISBN 1-58852-107-9

[61] 'Secton 2: Definitions - Information Tech. Law' (*Information Tech. Law*, 2020) <https://www.itlaw.in/secton-2-definitions/.>

[62] 'Certifying Authorities - Digital Signature Certificates' (*Digitalsignaturesale.com*, 2020) <http://www.digitalsignaturesale.com/certifying-authorities/.>

"Cyber Café" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public. (Section 2(1) (na) of the IT Act, 2000)

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. (Section 2(1) (nb) of the IT Act, 2000)

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3. (Section 2(1) (p) of the IT Act, 2000)

"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule of the IT Act, 2000 and includes digital signature. (Section 2(1) (ta) of the IT Act, 2000)

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Section 2(1) (w) of the IT Act, 2000)[63]

"Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary. (Section 2(1) (za) of the IT Act, 2000)

1.7 INTERDISCIPLINARY LAWS WITHIN CYBER LAW

The Government of India took effective steps for the development of information systems and the utilization of information resources after the *Information Communication Technology* revolution which commenced in 1975. Prior to that, there was no statute governing cyber laws which involved privacy, jurisdiction and issues of intellectual property rights and other legal issues. When the need arose of strict statutory laws to regulate the unlawful and illicit activities

[63]'ROLE OF INTERMEDIARIES IN THE INTERNET WORLD (Def-005) – THE CYBER LEGAL' (*Thecyberlegal.com*, 2020) <http://thecyberlegal.com/2019/09/15/role-of-intermediaries-in-the-internet-world/.>

in the cyber world and to protect the true meaning of technology, the "Information Technology Act, 2000" (ITA) heralded the new cyber law regime in the country.[64] The IT Act was passed and enacted by the Parliament of India on 17th October, 2000, comprising of 94 Sections and 2 Schedules to secure e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

The main objective of the Act has been to provide legal infrastructure for all the transactions carried out by means of electronic data interchange and other means of electronic communication.[65] It also aims to provide legal sanctity to all the electronic records and other activities carried out by electronic means. The Act essentially deals with the following issues:[66]

- Legal Recognition of Electronic Documents and Digital Signatures
- Offences and Contravention
- Justice Dispensation Systems for cyber crimes

The said act has also amended:

- *The Indian Penal Code, 1860*
- *The Indian Evidence Act, 1872*
- *The Bankers' Book Evidence Act, 1891*
- *The Reserve Bank of India Act, 1934*

Despite the above-mentioned amended acts, the IT Act itself specifies the acts which have been made punishable. The following statutes lay down provisions pertaining to securing digital signatures and electronic records.

- *The Information Technology (Certifying Authorities) Rules and Cyber Regulations Appellate Tribunal (Procedure) Rules* which came into force on 17th October, 2000
- *The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules* passed on 17th March, 2003
- *The Information Technology (Security Procedure) Rules* passed on 29th October, 2003.

[64]Dhall, S C "Need a Law to Tackle CYBER CRIME" Alive, no 396, Delhi Press, Oct 2015, p 64
[65]"India : Mandate to Govern E-Commerce Industry" MENA Report, Albawaba(London) Ltd, Feb 2017
[66]'IT Act 2000 – Penalties, Offences With Case Studies - Checkmate' (*Checkmate*, 2020) <https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/.>

Some Important Provisions under The Information Technology Act, 2000[67]

SECTIONS	OFFENCES	PENALTIES
Section 65	Tampering with computer source documents	Imprisonment up to 3 years or fine up to 2 lakh rupees or both.
Section 66	Hacking the computer system with intent or knowledge	Imprisonment up to 3 years or fine up to 2 lakh rupees or both.
Section 66B	Misappropriation of information stolen from computer or any other electronic gadget	Imprisonment up to 3 years or fine up to 1 lakh rupees or both.
Section 66C	Stealing someone's identity	Imprisonment up to 3 years or fine up to 1 lakh rupees
Section 66D	Accessing personal data of someone with the help of computer by concealing their identity	Imprisonment up to 3 years or fine up to 1 lakh rupees
Section 66E	Breach of Privacy	Imprisonment up to 3 years or fine up to 2 lakh rupees or both.
Section 66F	Cyber Terrorism	Imprisonment which may extend to imprisonment of life.
Section 67	Publication of obscene information in e-form	Imprisonment up to 5 years and fine up to 1 lakh rupees.
Section 67A	Publishing or circulating sex or pornographic information through electronic means	Imprisonment up to 7 years or fine up to 10 lakh rupees.
Section 67B	Publication or broadcast of such objectionable material from electronic means, in	Imprisonment up to 5 years or fine up to 10 lakh rupees.

[67]<https://www.tutorialspoint.com/information_security_cyber_law/offences_and_penalties.htm.>

	which children are shown in obscene mode	
Section 68	Failing to comply with the directions of the controller	Imprisonment up to 3 years or fine up to 2 lakh rupees or both.
Section 71	Misrepresentation	Imprisonment up to 2 years or fine up to 1 lakh rupees or both.
Section 72	Breach of confidentiality and privacy	Imprisonment up to 2 years or fine up to 1 lakh rupees or both.
Section 72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years or fine up to 5 lakh rupees or both.
Section 73	Publishing false digital signature certificate and false in certain particulars	Imprisonment up to 2 years or fine up to 1 lakh rupees or both.
Section 74	Publication for fraudulent purposes	Imprisonment up to 2 years or fine up to 1 lakh rupees or both.

The Information Technology Act, 2000 was further amended in the form of *Information Technology (Amendment) Act, 2008* which introduced 8 new cyber offences.

1.8 INTERNATIONAL FRAMEWORK OF CYBER LAW

Cyber law has been constantly evolving ever since its inception. One of the greatest concerns in the field of cyber law is the absence of a well-defined and exhaustive framework of law across the globe.[68] There was essentially no written record of progression in this field until 1960, with the publication of the first legal article on computer law titled as, *"A Lawyer's Guide through the Computer Maze"* by Roy N. Freed. Today's Internet was built-in in the early 1960's while the initial efforts for its regulation can only be recognized in the late 1990's. The first major attempt

[68] Flanagan,anne 2005 The law and computer crime: Reading the Script of Reform. International Journal of Law and Information Technology, 13, no 1: 98-117

was taken under the auspices of the Organization for Economic Co-operation and Development (OECD), who had published a report in the year 1986, listing five categories of offences that could be considered to be constituting a common approach towards computer crime.In addition to that, The Council of European Union approved the EU Data Protection Directive on July 20, 1995 and provided guidance that they "shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data". A step to bridge the digital gap between developed and least developed countries can be traced back to 1996, publication of the United Nations Commission on International Trade Laws (UNCITRAL) Model Law and 1998, the starting of the United Nations Conference on Trade and Development (UNCTAD) global campaign to promote e-commerce especially in developing countries. The UNCITRAL was created to streamline, harmonize and unify the law of International trade. A draft of 'Model Law' was prepared after foreseeing the inadequacies and impediments that had crept in the law affecting trade. The Model Laws which have been embraced by UNCITRAL pertaining to electronic commerce and electronic signature are:

a) Model Law on Electronic Commerce 1996

b) Model Law on Electronic Signature 1998-2001

The above-mentioned model laws have played a phenomenal role in the preliminary enactment of electronic laws in various countries. WIPO Copyright Rules 1996 and WIPO Performance and Phonograms Treaty Rules 1996 govern copyright infringements and trademark issues at national and international levels. Envisaging the issues relating to cybersquatting, on October 24th, 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) approved its Uniform Domain Name Dispute Resolution Policy, for the purpose of resolving domain name disputes.

The Convention on Cybercrime,[69] also known as the Budapest Convention on Cybercrime is the first international treaty which addressed computer crime and internet crimes. The Convention and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8th November 2001.[70] The Convention mainly aimed at:

[69]Gordon, Sarah, and Richard Ford. 2006.On the definition and classification of cybercrime. Journal in Computer Virology, 2, no. 1: 13-20

[70] Keyser, Mike. 2003. The Council of Europe Convention on Cybercrime. Journal of Transnational Law & Policy, 12, no 2: 287-326

- Harmonizing the domestic criminal substantive law elements of offences and provisions connected in the field of cybercrime.
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences committed by means of a computer system or evidence associated with is in electronic form.
- Setting up a fast and efficient regime of international co-operation.

Different countries have had their own experiences at the time of framing and implementing cyber laws. By and large, there are many convoluted legal issues that the law enforcement agencies of different countries have witnessed from time to time and which still remain unresolved. The legislators of law on cyberspace have faced eccentric obstacles in adapting the legal principles of the traditional legal systems.

1.9 LET'S SUM UP

In this unit we have studied the need and concept of cyber space along with its jurisprudence. We have seen the important terms that needs to be noted in cyber law and the interdisciplinary laws in cyber law. Finally, we have ended our discussion with the international framework of cyber law.

1.10 FURTHER READING

- Michael D. Scott, *Scott on Information Technology Law*, Vol. 1, preface xxx, Aspen publishers, U.S.A., 3rd edn.,2007.
- R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law*, 617, Kamal Law House, Kolkata, 2009
- http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1996.tb00056.x/full.
- Compliance With Information and Communication Technology Related Multilateral Frameworks : InformationTechnology Enabling Legal Frameworks for the Greater Mekong Sub- region, *74, Economic and SocialCommission for Asia and Pacific, United Nations Publication, 2004.*

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the various statutes associated with cyber laws in India?

A. The various statutes dealing with cyber laws in India are as follows:

- **a.** Information Technology Act, 2000
- **b.** The Indian Penal Code, 1860
- **c.** The Indian Evidence Act, 1872
- **d.** The Bankers' Book Evidence Act, 1891
- **e.** The Reserve Bank of India Act, 1934

2. What are the major areas of concern associated with and addressed by cyber laws?

A. The major areas of concern associated with and addressed by cyber laws deal with cyber crimes, electronic and digital signatures, intellectual property rights associated with cyberspace, data protection, data privacy etc.

3. Why is cyber law necessary?

A. In today's age of digitization, technology has gotten advanced to the extent wherein misuse of cyberspace can be done by one and all through various easily-accessible means and modes. Such misuse can give rise to issues of various magnitudes from violation of individual privacy and to threatened national security. Cyber laws which aim at addressing all such relevant issues are necessary for putting in place preventive measures for addressing them.

4. What are the international legal frameworks dealing with cyber laws?

A. The international legal frameworks dealing with cyber laws are EU Data Protection Directive, United Nations Commission on International Trade Laws (UNCITRAL) Model Law and 1998, United Nations Conference on Trade and Development (UNCTAD), Model Law on Electronic Commerce 1996, Model Law on Electronic Signature 1998-2001, Budapest Convention on Cybercrime.

5. What is the jurisprudence of cyber law?

A. The jurisprudence of cyber law deals with observing cyber uniform rules and policies at an international level and with curbing all the unlawful and illicit activities through enforcement of laws.

1.12 ACTIVITY

Explain the concept *'Cyber space as a metaphor'*. How would you show that the *'property in real space'* is compared with *'property in virtual space'*.Write in about 1000 -1500 words.

Unit 2: History and Emergence of Cyber Law

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Genesis of Information Technology Act

1.4 Indian cyber law regime

1.5 Critical Analysis of I.T. Act, 2000

1.6 Subsequent developments

1.7 Information Technology (Amendment) Act, 2008

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand

- Genesis of Information Technology Act
- Indian cyber law regime
- Information Technology (Amendment) Act, 2008

1.2 INTRODUCTION

In the early 1970s, countries began to adopt broad laws which were proposed to protect individual privacy. Most of the laws were based on the models introduced by the ***Organization for Economic Cooperation and Development(OECD)and the Council of Europe.***[71] The genesis

[71]Kavanagh, Camino "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace - Papers, Carnegie Endowment for International Peace, 28 Aug 2019

of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). In the U.S.A., the first federal computer crime statute was the Computer Fraud and Abuse Act, 1984. The fact that only one indictment was ever made under the Act before it was amended in 1986 shows how difficult it is to write effective computer crime legislation.[72]

1.3 GENESIS OF INFORMATION TECHNOLOGY ACT

The United Nations Commission on International Trade Law (UNCITRAL)adopted the ModelLaw on Electronic Commerce in 1996 in order to bring uniformity in the law of different countries.[73] The General Assembly of the United Nations by ***Resolution No. 51/162, dated 30th January 1997,*** recommended that all the States should give favorable considerations to this Model Law when they enact or revise their laws.

The Ministry of Commerce, Government of India created the first draft of the legislation following these guidelines termed as *"***E-Commerce Act 1998***"*. Since, later a separate ministry for Information technology came into being, the draft was taken over by the new ministry which re-drafted the legislation as ***"Information Technology Bill 1999".*** This draft was placed in the Parliament in December 1999 and passed in May 2000. After the assent of the President on June 9, 2000, the act was finally notified with effect from October 17, 2000, vide notification number G.S.R 788(E).

1.4 INDIAN CYBER LAW REGIME

The Information Communication Technology revolution in India began in 1975[74] when the Government of India strategically decided to take effective steps for the development

[72]SANS Institute Information Security Reading Room
<https://www.sans.org/reading-room/whitepapers/legal/federal-computer-crime-laws-1446>
[73]Meaning and Scope of information Technology Act
<https://theintactone.com/2019/05/07/bl-u4-topic-5-meaning-and-scope-of-information-technology-act/>
[74]Cyber laws regarding hacking in India – Lexlife
<https://lexlife.in/2020/03/18/cyber-laws-regarding-hacking-in-india/>

of information systems and the utilization of information resources. The National Informatics Centre under the Electronic Commission/Department of Electronics was the outcome of this view and was assisted by the United Nations Development Program (UNDP).[75] The formation of National Association of Software Services Companies in the early 1990s reflects on India's strength in this sector. Internet in India developed in 1995 and almost after 5 years, India took efficient steps to legislate its first cyber law.

The ***Information Technology Act, 2000***heralded a new cyber law regime in the country. With the advancement in changes, India became the 12th nation in the world to enact cyber laws. As outlined in the preamble of the I.T. Act, 2000, the objectives of the Act is to provide legal recognition for E-commerce transactions, facilitate Electronic Governance and to amend the Indian Penal Code, Indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The Act also establishes a regulatory framework for cyber laws and lays down punishment regimes for different cyber crimes and offences.

Although the enactment of the Information Technology Act followed the UNCITRAL Model law to a considerable extent, there are, however, some areas where the I.T. Act departs from the Model Law. The deviations which were explored are quite distinct from the Model law in two key areas: digital signatures and provisions relating to online contracting. These deviations were carried out keeping in mind the legal and economic conditions prevailing in the country.

1.5 CRITICAL ANALYSIS OF THE I.T. ACT, 2000

With the enactment of the Information Technology Act, 2000, in India, law has taken a quantum jump to include even the intangibles under its purview. The Act is a proactive piece of legislation. It is to be read and understood from the point of view of *one*, facilitating international trade and *two*, as an alternative to paper-based methods of communication and storage of information. The Act is not only in tune with the UNCITRAL's Model Law on Electronic Commerce but it also unfolds various aspects of information technology to promote efficient delivery of Government services by means of reliable electronic records. The application of the

[75] An overview of cyber-crimes and cyber law in India <https://www.grin.com/document/456973>

Information Technology Act rests with the courts. It is a settled principle that the interpretation of a provision of law relates back to the date of the law itself and cannot be prospective from the date of the judgment because concededly that court does not legislate but only gives an interpretation to existing law.[76]

It was held that, a statute is an edict of the legislature. The language employed in a statute is the determinative factor of legislative intent. Words and phrases are symbols that stimulate mental references to referents.[77] The object of interpreting a statute is to ascertain the intention of the legislature enacting it.[78]

The fact is, that judiciary has always been able to assimilate technology and as the Supreme Court has observed in ***SIL Import. USA v Exim Aides Silk Importers,***[79]the need of the judiciary to interpret the statute by making allowances for any relevant technological change that has occurred. In ***Grid Corpn. of Orissa Ltd. V AES Corpn.,***[80]it was held by the Supreme Court that *"when an effective consultation can be achieved by resort to electronic media and remote conferencing, it is not necessary that the two persons required to act in consultation with each other must necessarily sit together at one place unless it is the requirement of law or of the ruling contract between the parties".*

Similarly, in ***State of Maharashtra v Dr.Praful B. Desai,*** [81] it was held that *'**videoconferencing'***is an advancement in science and technology which permits one to see, hear and talk with someone far away, with the same facility and ease as if he is present before you i.e., in your presence. In video-conferencing, both parties are in presence of each other. Thus it is clear that so long as the accused and / or his pleader are present when evidence is recorded by video-conferencing that evidence is being recorded in the ***'presence'***of the accused and would thus fully meet the requirements of Section 273 of the Criminal Procedure Code. Recording of such evidence would be as per *'procedure established by law'*. Also in ***Amitabh bagchi v***

[76]Lily Thomas v. Union of India – My Legal Partner.
<https://mylegalpartner.wordpress.com/2018/05/23/lily-thomas-v-union-of-india/>
[77]Intent: The Object of Interpretation - Blogger
<https://lawaids.blogspot.com/2010/05/intent-object-of-interpretation.html>
[78]*Institute of Chartered Accountants of India v Price Waterhouse*, AIR [1998] SC 74
[79]*SIL Import. USA v Exim Aides Silk Importers*AIR [1999] SC 1609
[80]*Grid Corpn. of Orissa Ltd. v AES Corpn* [2002] 7 SCC 736
[81]*State of Maharashtra v Dr. Praful B. Desai* AIR [2003] SC 2053

Enabagchi, [82] **and in** ***BodalaMurali Krishna v Smt. BodalaPrathima,*** [83] the facility of video-conferencing was allowed.

Thus it is clear that, the Supreme Court approves of the principle of updating construction, i.e., law must constantly be on the move adapting itself to the fast-changing society and not lag behind. Moreover, the Supreme Court is advocating use of external aids to gather information. In ***Ponds India Ltd. v Commissioner of Trade Tax, Lucknow,*** [84] the Court mentioned that *'Wikipedia, like all other external aid to construction, like dictionaries etc. is not an authentic source, although the same may be looked at for the purpose of gathering information'*. In ***CIT v Associated Distributers Ltd.,*** [85] the Court had taken the meaning of ***'bubblegum'*** given in Wikipedia.

In the view of the fact that every second case now requires appreciation of electronic evidence on the part of the judge, it thus becomes imperative that a judge needs to wear a hat of technocrat as well! Applying technology and getting desired results is one thing, but appreciating the value of the *'evidence'* is another. One may lose evidence not because of *'lack of technology'*, but because of *'lack of appreciation of technology'*. Hence, the questions before the Court of law are:

- Did the investigators / litigants take care in gathering the evidence? and
- Could they fake the evidence?

As the Supreme Court has held in ***KajalSen v State of Assam,*** [86] that *'it is a duty of the court to appreciate evidence minutely, carefully, and to analyze it'*.In this context, it is interesting to note that in ***Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra,*** [87] the Supreme Court appreciated the electronic evidence, whether in the form of CCTV footage, mobile device, memory cards, data storage devices, intercepted communications over VoIP, IP Addresses, etc. while delivering the judgment.

[82] *Amitabh bagchi v Enabagchi* AIR [2005] Cal 11
[83] *BodalaMurali Krishna v Smt. BodalaPrathima* AIR [2007] AP 43
[84] *Ponds India Ltd. v Commissioner of Trade Tax, Lucknow* [2008] 8 SCC 369
[85] *CIT v Associated Distributers Ltd* [2008] 7 SCC 409
[86] *KajalSen v State of Assam* AIR [2002] SC 617
[87] *Mohammed Ajmal Mohammad Amir Kasab v State of Maharashtra* AIR [2012] SC 3565

The Information Technology, 2000 was brought to light mainly to ensure legal recognition of e-commerce in India. The provisions solely pertained to establishing digital certification processes within the country. 'Cyber Crime' as a term was taken off the books i.e., it wasn't defined in the Act. It only delved with a few instances of computer-related crimes.

Experts pointed out several flaws in the I.T Act, 2000. They were as follows:-

- The Act failed to provide any provisions regarding domain names and resolving disputes on such names.
- The Act did not explain how cyber crimes affecting computers in India committed from outside India using the Internet were to be handled.
- Many cyber crimes were not defined in the Act such as cyber defamation, cyber stalking and cyber harassment.
- The Act did not cover the privacy and protection of personal data such as medical records.
- Lastly, the Act neglected to deal with regard to Intellectual Property Rights and provide provisions to punish persons or organizations sending unsolicited emails.

It has been argued that the Act of this nature would divide society into *digital haves* and *digital have-nots.* This argument is based on the premise that with an extremely low PC penetration, poor Internet connectivity and other poor communication infrastructure facilities, a country like India would have islands of *'digital haves'* surrounded by *'digital have-notes'*. Logically speaking, such an argument is untenable as the *'digital core'* has been expanding horizontally and everyday communication connectivity is rising across India. The country is one its way to become a *'one-wired nation'*.

1.6 SUBSEQUENT DEVELOPMENTS

1.	**Information Technology (Certifying Authorities) Rules, 2000**	These rules prescribe the eligibility, appointment and working of Certifying Authorities (CAs). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended

		in 2003, 2004 and 2006.[88]
2.	**Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000**	These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.[89]
3.	**Information Technology (Certifying Authority) Regulations, 2001**	They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first was the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act and Secondly, The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.
4.	**Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002**	The IT Act was amended by the Negotiable Instruments (Amendments

[88]CH Magazine | Need for Cyber Law <https://www.chmag.in/articles/legalgyan/need-for-cyber-law/>

[89]These rules were amended in 2003 2004 and 2006 <https://www.coursehero.com/file/p4vpcvd/These-rules-were-amended-in-2003-2004-and-2006-Note-The-Act-rules-regulations/>

		and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques.[90]
5.	**Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003**	These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers. The appointment of adjudicating officers to decide the fate of multi-crorecyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws.[91]
6.	**Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004**	They prescribe provisions relating to secure digital signatures and secure electronic records.[92]

1.7 INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

[90]Introduction to Indian Cyber Law <http://www.osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf>

[91]UNIT 7: Information Technology Rules Notified <https://alayalegal.com/unit-7-information-technology-rules-notified-under-the-information-technology-amendment-act-2008/>

[92]The Information Technology (Use of Electronic Records) <http://www.lexcyberia.com/pdf/The%20Information%20Technology%20(Use%20of%20Electronic%20Records%20and%20Digital%20Signatures)%20Rules,%202004.pdf>

Based on the criticism and experience gained by using the Information Technology Act, 2000, the Government set up an expert committee to review the I.T. Act in January 2005. The committee had representatives from the Government, IT Industry and legal experts and submitted its report in August, 2005. The IT (Amendment) Bill 2006, was introduced in the LokSabha on December 15, 2006, by the Union Minister of State for Communication. The 2006 Bill was modified and passed by the Parliament on 23-12-2008. It was notified after the assent of the President on 05-02-1009 as the Information Technology (Amendment) Act, 2008, (Central Act No. 10 of 2009).[93]

With the enactment of the Amended Act, the following rules came into force:-

- Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.[94]
- Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
- The Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009.
- Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity ofChairperson and Members) Rules, 2009.

1.7 CHANGES INTRODUCED BY THE AMENDED ACT

The Information Technology (Amendment) Act, 2008 is a substantial addition to India's Information Technology Act, 2000. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed

[93]UNITE INDIAN HACKERS.
<https://unitehackers.blogspot.com/>
[94]National Seminar on Enforcement of Cyberlaw, New Delhi
<https://cyberlawsconsultingcentre.com/wp-content/uploads/IT-Act-2000-vs-2008.pdf>

through it, and making corporations responsible for implementing effective data security practices and liable for breaches. The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.[95]

There are also challenges posed by the amended Act that can be foreseen and our country needs to be well equipped to overcome these challenges. The role of Adjudicating Authority in the amended Act is very significant. The subject matter of its jurisdiction, adjudging matters alleging contravention and awarding compensation under *chapter 9* is explained in clearer terms in the Amended IT Act. The amended Act also curtails the power & jurisdiction of the Adjudicating officers and excludes those matters where compensation claimed is more than 5 crores.

The Information Technology (Amendment) Act, 2008 introduced eight new cyber offences.[96]

- Sending offensive messages through a computer or mobile phone (Section 66A)
- Receiving stolen computer resource or communication device (Section 66B)
- Punishment for identity theft (Section 66C)
- Punishment for cheating by personation using computer resource (Section 66D)
- Punishment for violating the privacy or video voyeurism (Section 66E)
- Cyber Terrorism (Section 66F)
- Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A)
- Child pornography (Section 67B)

1.8 LET'S SUM UP

In this unit we have studied the genesis of information technology act along with the critical analysis of the I.T. Act, 2000 that gives you the drawbacks in the act. We have ended our discussion with the subsequent developments and the changes that were brought in the I.T. (Amended) Act, 2008.

[95] What is Information Technology Amendment Act 2008 <https://whatis.techtarget.com/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008>

[96] Full text of "A Text book of cyber crime and penalties" <https://archive.org/stream/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali_djvu.txt>

1.9 FURTHER READING

- http://gilc.org/privacy/survey/intro.html.
- R.K. Bagga, Kenneth Keniston (eds.), et. al., *The State, I.T. and Development*, 137, Sage Publications India Pvt. Ltd. , New Delhi, 2005.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Briefly describe the genesis of cyber laws?**

A. The basis of Cyber laws can be traced back to the laws on privacy based on the models introduced by the Organization for EconomicCooperation and Development (OECD) and the Council of Europe. However, the first laws on data protection were laid down in Germany in 1970, followed closely by the national laws in Sweden (1973), the United States(1974), Germany (1977) and France (1978) until 1984, when the USA came up with the first federal computer crime statutewas the Computer Fraud and Abuse Act. In 1996, The United Nations Commission on International Trade Law (UNCITRAL) adopted the ModelLaw on Electronic Commerce which subsequently paved the way for the Information Technology Bill, 1999 and then the Information Technology Act, 2000 in India.

2. **What are the new provisions of the Information Technology (Amendment) Act, 2008 amended following the amendment of the Information Technology Act, 2000?**

A. The provisions of the Act after amendment are as follows:

-Sending offensive messages through a computer or mobile phone (Section 66A)

-Receiving stolen computer resource or communication device (Section 66B)

-Punishment for identity theft (Section 66C)

-Punishment for cheating by personation using computer resource (Section 66D)

-Punishment for violating the privacy or video voyeurism (Section 66E)

-Cyber Terrorism (Section 66F)

-Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A)

-Child pornography (Section 67B)

3. How is the Negotiable Instruments Act related to the concept of cyber crimes?

A. The Negotiable Instruments Act deals with the concepts of electronic cheques and truncated cheques and is hence related to the concept of cyber crimes.

4. What were the drawbacks in the Information Technology Act, 2000, for which the amendment had to be introduced?

A. The drawbacks in the Information Technology Act, 2000 for which the amendment act of 2008 was introduced are as follows:

- The Act failed to provide any provisions regarding domain names and resolving disputes on such names.
- The Act did not explain how cyber crimes affecting computers in India committed from outside India using the Internet were to be handled.
- Many cyber crimes were not defined in the Act such as cyber defamation, cyber stalking and cyber harassment.
- The Act did not cover the privacy and protection of personal data such as medical records.
- Lastly, the Act neglected to deal with regard to Intellectual Property Rights and provide provisions to punish persons or organizations sending unsolicited emails.

5. Name the major rules and regulations associated with the Information Technology Act, 2000 that deal with cyber laws?

A. The major rules and regulations associated with the Information Technology Act, 2000 that deal with cyber laws are as follows:

- Cyber Regulations Appellate Tribunal (Procedure) Rules,2000
- Information Technology (Certifying Authority)Regulations, 2001
- Information Technology (Qualification and Experience ofAdjudicating Officers and Manner of Holding Enquiry) Rules, 2003
- Information Technology (Use of Electronic Records andDigital Signatures) Rules, 2004

1.11 ACTIVITY

How would you summarize the aims, objectives, salient features and critical analysis of Information Technology Act, 2000? Write in about 1000 words.

Unit 3: Outreach and Impact of Cyber Law

3

SUBJECT CODE: 101

CYBERSPACE AND ITS GOVERNANCE

BLOCK 2 – FUNDAMENTALS OF CYBER LAW

UNIT 3 – OUTREACH AND IMPACT OF CYBER LAW

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Outreach

1.4 Concrete Global Development

1.5 Prevention of Cybercrime

1.6 Efficacy of the existing cyber law

1.7 Positive and Negative Impacts of Cyber Law: The Way Ahead

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand

- The far-reaching impacts of cyberlaw as a concept
- The ways and means of preventing cybercrimes and the active international contribution towards it

- The positive and negative impacts of cyber law and the way ahead

1.2 INTRODUCTION

In today's world, cybersecurity has become a global phenomenon affecting people across the world and creating complex social and technical challenges for governments to face. In spite of the all-pervasive presence of cyberspace and the undeniable significance of its influence across one and all, genuine awareness regarding its scope and outreach is still limited and has not sufficiently reached people at large. In spite of the large number of cyberattacks occurring every day, people tend to believe that the internet offers an invariably safe and harmless platform for use.[97] Some of the few challenges pertaining to cyber law include the ambiguities involved in the concept and the complexity linked with the social and technological aspects of cyber law. The need of the hour is to create awareness for cyber law and ensure that common people are introduced to the concept and subject-matter of cyberspace, cyber law and cybercrimes extensively. The dependence of life and various aspects thereof on cyberspace is increasing by the day. The intangibility of cyberspace, the multifaceted properties make it all the more difficult to address all the limbs of the subject matter of cyber law.[98]

1.3 OUTREACH

The growth and development of cyber law have overcome territorial boundaries and made geographic limitations irrelevant. While on one hand, it has helped foster connectivity and communications become easier and faster at a cheaper price and for better convenience, on the other, it has helped criminal activities grow on an international level. In acknowledgement of the significance of cyber law as well as its impacts, countries are not only introducing specific legislation to address the concept and its potential effects, existing frameworks of law are also being extensively amended to incorporate various facets of cyber laws.[99] As per reports, in over 90 percent instances, activities relating to cybercrime get noticed and detected only when reports

[97]Buono, L Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum* 15, 1–8 (2014) <https://doi.org/10.1007/s12027-014-0333-4>

[98]Salane, D and Misshula, E (to appear 2014) "Legislative and Regulatory Attempts to Control Cybercrime: The Good, the Bad and the Ugly"

[99]Salane, D (2013, July 31) "The Case for Strong Data Breach Notification Legislation"

are filed by victims, both individual and corporate entities and that over 80 percent instances of cybercrimes involving individual victims go unreported. Such underreporting primarily stems from lack of awareness amongst people regarding cyberspace as a whole, which in turn result in causing and creating victim shaming. It is necessary that every case of cybercrime in given specific significance and dealt with in an incident-driven approach towards every such crime committed. Likewise, law enforcement must mandatorily include both aspects of traditional techniques as well as new policies developed to incorporate modern procedural provisions. Stanford Research Institute (SRI) was first to suggest a prototype in 1973 which has by and large been followed by writers on cybercrime. The organizing schema suggested was; the computer as a subject of a crime; the computer as an object of a crime; or the computer as instrumentality. The increasing use of other devices like the cell phone or PDA required reformulation of the concept.[100] The evolving definition of cybercrime needs to accommodate the mobile phone broadband communication, wireless networks and the Internet. The definition should accommodate both current and emerging technologies.

1.4 CONCRETE GLOBAL DEVELOPMENT

Many countries across the world have enacted their own criminal laws, computer laws, information technology laws and intellectual property laws etc. to prevent and combat the cyber criminality. In view of the international dimension of cybercrime, the problem of jurisdiction arose particularly where the nationals or corporations of two or more than two countries were involved in the crime or where the criminal belongs to a different nationality and the crime was committed in a different country.[101] The crucial problem, therefore, is that the law of which country is to be applied to resolve the dispute or to try the criminal(s), particularly when there is a variation in the cyber laws and penal laws of different countries. Internet is a vast global network of computers and the feasibility of the cybercriminals to perpetrate the crime from one destination and committing the crime at other destination with anonymity urgently requires development of a universal and uniform law governing and regulating the cyberspace

[100]Brenner, Susan W and Bert-JaapKoops (2004) Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, Vol4(1), 1-46

[101]Maras, Marie-Helen (2014) *Computer Forensics: Cybercriminals, Laws and Evidence*, Second edition. Jones and Bartlett

transactions to resolve the issues of cyber criminality by mitigating the jurisdictional problem and the conflict of laws. The ever increasing phenomenon of cybercrime calls for immediate concerted efforts on the part all the countries, institutions, industries, technocrats and jurists alike to come up with universally uniform law so that the common criminals of mankind may be tried and punished without the legal and jurisdictional hassles. In this direction the international community is taking the resolute efforts to address the problem of international cyber criminality.

Global development in this direction began with the 12th Conference of the Directors of ***"Criminological Research Institutes"***of the Council of Europe, which discussed computer-related crimes for the first time in 1976. As a sequel to this conference, the Select Committee of the Council of Europe on economic Crime conducted a study of economic crime in general and made its recommendations on the same. In 1983, the ***Organization for European Co-operation and Development (OECD)***undertook a study on the harmonization of international criminal laws, which resulted into the publication of the report entitled "Computer Related Crime – Analysis of Legal Policy" in 1986.[102] The Report recommended a list of computer crimes that countries should consider prohibiting and penalizing by means of legislation:

- The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value;
- The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;
- The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;
- The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put in on the market;
- The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions.

[102]Maras, Marie-Helen *Cyberlaw and Cyberliberties* Oxford University Press, forthcoming, 2020

Subsequently, the Council of Europe initiated its own study on computer crime with a view to evolving guidelines to help legislators determine the nature and nuances of computer-related crime. The Committee of Ministers, of the Council of Europe, accepted these recommendations in September 1989. The business transactions are now being carried on in the cyberspace through the nets and the online transactions have opened new vistas for unscrupulous cyber criminals to defraud and cheat the genuine businessmen and consumers. In view of the growing menace of cybercrime, the United Nations Congress in its ***13th Plenary Session*** held in 1986, adopted a resolution calling up member States to intensify their efforts to combat cybercrimes through adequate legal measures.[103]

1.5 PREVENTION OF CYBERCRIME

Preventive measures are available that help deter cybercriminals, such as passwords, firewalls, encryption, and other security policies and procedures. Cybercrime detection is a necessary last line of defence regarding loss prevention or at least loss minimization. Detection techniques include tripwires, configuration-checking tools, and anomaly detection systems. A brief overview of each of these intrusion detection techniques follows:[104]

- A tripwire is software programs that take snapshots of critical system characteristics that can be used to detect critical file changes. Tripwires provide evidence of electronic crimes since most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics in the course of hacking the system.

- A configuration-checking tool also referred to as a ***"vulnerability assessment tool,"*** refers to software programs that detect insecure systems. Configuration-checking tools are primarily preventive in nature but used as a monitoring device they can also provide evidence regarding electronic crimes.

[103]Wall, David S (2007) *Cybercrime: The Transformation of Crime in the Information Age* Polity Press (2nd edition, forthcoming 2020)
[104]Kratchman, Stanley & Smith, Jacob & Smith, Murphy (2008) The Perpetration and Prevention of Cybercrimes

- An anomaly detection system focuses on unusual patterns of system activity. Anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in order to identify deviations from expected activity.

Cybercrime is unlikely to be identified from random and intensive searches for evidence of criminal activity.[105] If a cybercriminal can convince an intrusion detection system to continually and uselessly increase its use of computer resources, then the criminal has effectively accomplished denial of service, a particularly destructive type of cybercrime. In such a case, computer resources are wasted and cybercriminals are not detected. Since cybercrime is detrimental to business operations, business firms and their stakeholders clearly benefit from stopping cybercrime. Unless properly and continuously "fine-tuned," a single intrusion detection technique may tend to under-report cybercrimes or over-report such as excessive false alarms. In most cases, companies find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes.

The concept of prevention of cybercrimes[106] deals inter alia with strategies and schemes to tackle the scope and risks of occurrence of cybercrimes. To ensure sufficient measures are in place, countries implement national policies for the prevention of cybercrimes. About 40 to 50 percent countries across the world have actively recognized the necessity of establishing national policies and legislations to address cybercrimes and have acknowledged that introducing relevant legislations, developing an effective criminal justice system and spreading awareness about the concept would ensure prevention of its misuse.

With the rise in cybercrimes, research has now revealed that in most of the developing countries, individual users of internet take basic precautionary steps for securing themselves and their devices against cybercrimes. While on one hand, educating users has proved to be most effective, on the other, strengthening the societal and technological infrastructure for protection against acts of cybercrime has ensured that potential risks can be confronted. Appropriate actions must be taken by qualified professionals to successfully resolve cybercrime. Since some business

[105]Luehlfing, M, C Daily, T Phillips, and LM Smith 2003 Cyber Crimes, Intrusion Detection, and Computer Forensics Internal Auditing, 18:5 (September-October): 9-13

[106]Lakshmanan, Annamalai. (2019) Literature review on Cyber Crimes and its Prevention Mechanisms

firms may lack qualified computer security personnel, hiring outside professionals.[107] Law enforcement agencies can help with cybercrime investigations; although, many law enforcement agencies lack the technical expertise to investigate electronic crimes. Most can obtain warrants and seize computer equipment but may be unable to find the evidence needed to resolve the cybercrime.

1.6 EFFICACY OF THE EXISTING CYBER LAW

The IT Act, 2000 was amended by the IT (Amendment) Act, 2008. However, it is apposite to state that the Amendment Act could not address the legislative weaknesses of the law. This segment deals exclusively with the infirmities and shortcomings which the Amended Act is suffering from and to ascertain as to how the existing cyber law can be strengthened to make it efficacious and effective to counter the escalating menace of cybercrimes being committed against the individuals, institutions, society at writ large and the governments.[108]

While there are many legislations not only in many Western countries but also some smaller nations in the East, India has only one legislation-the I T Act, 2000. The IT Act, 2000, though a landmark legislation to deal with the cybercrime in India but the Act could not provide exhaustive measures to counter the rising trend in the cybercrime, for despite the amendment incorporated in it to attune it with the need to curb the cybercrime in view of the technological development in the area of information technology, a number of crimes and important issues have been left unaddressed. Many of the cyber crimes like cybersquatting with evil attention to extort money, Spam mails, ISP‘s liability in copyright infringement, data privacy issues have not been given adequate coverage in the legislative scheme of the Act. In order to make the Act efficacious and effective following measures need to be addressed:[109]

[107] National Cyber Security Centre (NCSC) 2017Cyber crime: understanding the online business model p 10 <https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity>

[108] Kumar, P. N. V. (2016). Growing cybercrimes in India: A survey. Proceedings of 2016 International Conference on Data Mining and Advanced Computing, SAPIENCE 2016, 246–251 <https://doi.org/10.1109/SAPIENCE.2016.7684146>

[109]Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore and Vasek. 2019 Measuring the Changing Cost of Cybercrime p 20 <https://weis2019.econinfosec.org/wp-content/uploads/ sites/6/2019/05/WEIS_2019_paper_25.pdf>

a) The Amendment Act of 2008 has failed to define the word ―Hacking‖ or ―Hacker‖, surprisingly the act of hacking with the very word ―hacking‖ finds a mention in section 66 of the original Act.

b) The new amendments under Section 43-A make it mandatory for corporate-possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices.

c) The IT Rules, 2011 framed under the Sec 43-A having subsection 8(2),8(3) and 8(4) which relates to the introduction of ISO 27001 as a mandatory compliance requirement through the backdoor with the use of misleading words mentioned in the rules. ISO 27001 Compliances and Audit now has additional compliance obligation for organizations.

d) Section 79 of the amended IT Act, 2000 is not a penal section under the Act. Penalty under the Act would arise on any person or a body corporate. When an incident has occurred on account of other sections such as Sec. 43, 43-A, 65, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 69, 69A, 69B, 70, 71, 72, 72A, 73, 74,84B, 84C etc. which can be brought under any of these sections and the person who is accused is otherwise an-Intermediary as defined under the Act, then the provisions of Section 79 apply. These provisions give him an opportunity to escape his liability. To use these provisions he needs to act such in a manner which can be considered as-exercising Due Diligence. The privileged intermediaries include telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

e) The amended IT Act, 2000 has not specifically dealt with the issue pertaining to e-discovery. Today, organizations are relying increasingly upon digital evidence like email etc. and media as a means of communicating with each other and conducting business. IT Act, 2000 remains silent on this issue and also leave scope for business exploitation of e-discovery by large consulting firms at their own interpretation.

f) A Cyber Café is also a - Intermediary hence the obligations under Section 79 and the rules framed therein for - Intermediaries already apply to Cyber Cafes. The rules for Cyber Cafes are incomplete rules requiring further rules making at the State Government

level. The rules also infringe on the power of the State Government for maintaining law and order in the State.

g) Taxation of ecommerce transactions when a transaction is committed from Indian jurisdiction is not explicitly discussed nor is any passing reference made with a view to bind it with Indian tax law.

h) A clear section with regards to Jurisdiction of courts over parties staying or operating in different jurisdictions or countries is not covered. Even though having a complete separate legal jurisdiction for the cyber world, is not an expectation but certain clear guidelines necessary help lower courts and humble netizens.

i) Major offences covered under this Act are bailable. Thus interim reliefs, anticipatory bails etc. would be in a vogue with cyber criminals.

1.7 POSITIVE AND NEGATIVE IMPACTS OF CYBER LAW: THE WAY AHEAD

The gradual growth of cyber law and cyberspace over the years has brought to the fore both positive and negative aspects of the concept. It cannot be denied that owing to the vast outreach of cyber law as a concept, fighting its negatives and utilizing its positives require a multi-layered approach, which in turn demand an extensive and comprehensive understanding of the subject matter itself.[110]

While the positive impacts of cyberspace include advancement to the effect of dissolving territorial limitations, the negatives inter alia include the threat of organized cybercrime, which, arguably, acts as the biggest hazard to global banking.

Undeniably, the massive ambit of the subject itself demands that the regulations controlling it are multi-faceted. The following lists down the probable ways of controlling the effects and impacts of cyberspace.

- Ensuring that there are territorial as well as global laws to address disputes arising from use of cyberspace

[110]Presented at the International Conference: Global Perspectives on Justice, Security and Human Rights, John Jay College of Criminal Jutice, June 6-9

- The imposition of deterrent penalties to ensure the prevention of such crimes being committed
- Co-operation and inter-relationship established between various limbs of society such as firms, governments etc., for the purposes of strengthening measures of cybersecurity.

1.8 LET'S SUM UP

In this unit we have studied impacts of cyber law along with the ways and means to prevent cybercrimes and the active international contribution towards it. We have ended our discussion with the efficacy of the existing cyber law and elucidating the positive and negative impacts of cyber law.

1.9 FUTHER READING

- Donn B. Parker, S Nycum and S.S. Oura, Computer Abuse (Mento Park,, California Standford Research Institute, 1973).
- AmitaVerma, Cyber Crimes & Laws, Central Law Publication, (2009) p. 354.
- Suresh T. Vishwanathan, "The Indian Cyberlaw", at 104 (2001).

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. How do cyber laws endeavor to prevent cyber crime?

A. Basic awareness regarding cyber laws has revealed through extensive research that in most of the developing countries, individual users of internet take basic precautionary steps for securing themselves and their devices against cybercrimes. Furthermore, cyber laws have also strengthened the societal and technological infrastructure for providing protection against acts of cybercrime and ensuring ways and means of confronting risks.

2. What are the major objectives of cyber laws?

A. The major objectives of cyber laws are as follows:
   - Ensuring that there are territorial as well as global laws to address disputes arising from the use of cyberspace
   - Imposing deterrent penalties to ensure the prevention of such crimes being committed
   - Co-operating with and establishing inter-relationship between various limbs of society such as firms, governments etc., for the purposes of strengthening measures of cybersecurity

3. What are the drawbacks of cyber laws?

A. The drawback of cyber law is that it fails to keep pace with the advancement in the technology which has now dissolved territorial limitations and has threatened to initiate organized cybercrime, which, arguably, acts as the biggest hazard to global banking.

1.11 ACTIVITY

Elucidate the global developments after the I.T. Act 2000 along with the preventive measures that needs to be taken with respect to cybercrimes? (800-1000 words)

Unit 4:Major Amendments in Various Statutes

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 The Information and Technology Act, 2000 – Relevance in Cyber Law

1.3 Genesis of the I.T. Legislation

1.4 Content

1.5 Relevance

1.6 Indian Penal Code – Relevance in Cyber Law

1.7 Cyberspace and the Law of Evidence

1.8 Bankers' Books of Evidence Act, 1891

1.9 Reserve Bank of India Act, 1934

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible Answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand

- The existing laws in the country addressing disputes and crimes related to cyberspace
- Various relevant provisions of the Information Technology Act, 2000 along with its amendment
- Various relevant provisions of the Indian Penal Code, 1860
- Various relevant provisions of the Indian Evidence Act, 1872
- Various relevant provisions of the Bankers' Books Evidence Act, 1891

1.2 THE INFORMATION AND TECHNOLOGY ACT, 2000 – RELEVANCE IN CYBER LAW

In the advanced society that we live in today, cybercrime is perceived as a phenomenon that is social and economic at the same time. Although cybercrimes are not defined in any legislation in India, nor the Information Technology Act, 2000, cybercrime is deemed to include any illegal activity that involves the internet, cyberspace or computers. The Information Technology Act along with the amendment of 2008 however address all the necessary ingredients that contribute towards the commission of cybercrime.

1.3 GENESIS OF THE I.T. LEGISLATION

The globalization of the 90's introduced a change in the economy which involved governance and growth of a society being computerized. As a result of this, international trade and commerce became dependent on electronic communication. Subsequently, the **United Nations Commission on International Trade Law (UNCITRAL)** was adopted in 1996 which acknowledged e-commerce and electronic records. To ratify and give effect to the provisions of the UNCITRAL, the Government of India enacted the Information Technology Act in 2000. Some of the unique features of the Act deal with –

- Legal recognition of electronic documents
- Legal recognition of digital signatures
- Addressing the commission of cybercrimes

The Information Technology Amendment Act, 2008 (ITAA) was passed to mark an end to all the controversies, disputes, debates and criticism arising from the nature of provisions in the IT Act. While some parts of the Act were considered draconian, others were marked as extremely dilute. The Amendment Act was hence introduced to incorporate extensive modifications into the existing Act by inter alia acknowledging the concepts of data privacy, information security, roles of intermediaries, cybercrimes like child pornography and cyber terrorism.

1.4 CONTENT

In acknowledgement of the necessity of adapting a system adept in dealing with the technological changes, the Act specifically defined the terms used in association with cyberspace, such as 'computer resource', 'communication device', 'data', 'information', 'security procedure', etc. While digital signature had been defined in the Act of 2000 as 'authentication of electronic record' using Public Key Infrastructure, the Amendment Act of 2008 gave it legal validity by re-defining it as 'digital signature and electronic signature' so as to ensure that the understanding of the term does not get dependent on the technical and technological aspects of the concepts.

The Act of 2000 further acknowledges under section 4 the validity of electronic records for recognition and maintenance of e-contracts. The Act also attempts to address data theft and misappropriation through its provisions, thereby adding a major component in the legislation. **Section 43** of the Act, the first legal provision in the country to elaborate on the civil aspects of data theft, lays down that any person accesses, downloads, copies, extracts, data from a computer or contaminates the data contained therein without the express authorization of the person owning or acting in charge of such computer shall have committed the civil offence of data theft and shall be liable to pay damages to any party affected as a result of such theft. While the Act of 2000 had capped the upper limit of such damage at Rs. 1,00,00,000/- (Rupees One Crore only), the Amendment Act of 2008 made it uncapped.

While Section 43 of the Act deals with the civil aspects of data theft, sections 65 and 66 address the criminality of such theft. Section 65 deals with computer source code being destroyed, damaged, concealed, altered or tampered with in any manner whatsoever, in contravention of the law to maintain such data. As per the Act, such offence will be punishable with imprisonment for upto three years and/or a fine of Rs. 2,00,000/- (Rupees Two Lakhs only). Section 66 addresses all acts of data theft as defined under Section 43 of the Act being with criminal intention of causing fraudulent and criminal activities and punishes such acts with imprisonment of upto three years and/or a fine of Rs. 5,00,000/- (Rupees Five Lakhs only). The Act of 2000 referred to

hacking of data within the ambit of Section 66, but the provision under the Amendment Act of 2008 eliminates such references to hacking. Additionally, a list of cognizable and non-bailable offences has been annexed to section 66 so as to widen its ambit, as listed out hereunder –

- Section 66A – addresses instances of offensive messages being sent to any device of electronic communication with the purposes of misleading or deceiving the recipient thereof regarding such message sent; whereby such instances are to be punished with imprisonment of upto three years or fine.
- Section 66B – deals with dishonest receipt of stolen computer resources or any other devices of e-communication, the punishment for which extends upto three years' imprisonment and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66C – concerns with theft of identity or personal information like electronic signature and password, and imposes a punishment of upto three years' imprisonment and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66D – is associated with the act of cheating by personation that involves a computer or any other device of e-communication, which shall entail a punishment of imprisonment for a term extendable upto three years and/or a penalty of Rs. 1,00,000/- (Rupees One Lakh only).
- Section 66E – deals with violation of privacy without the consent of the person concerned which shall involve entail a punishment of imprisonment for three years and/or a penalty of Rs. 2,00,000/- (Rupees Two Lakhs only)
- Section 66F – addresses cyber terrorism committed with the intention of causing unrest in the nation by threatening the security, sovereignty, unity and integrity of the country by either commission or omission of acts associated with the use and access to computer and other devices of e-communication. Acts of causing contamination in computer or e-communication devices likely to cause death/injury to people/ property shall fall within the ambits of this provision. The punishment imposed for such activities is life imprisonment.

Section 43A was introduced by the Amendment Act of 2008, to address instances wherein failure of data protection occurs owing to negligent approach towards maintenance of security

practices and thereby leads to payment of compensation. The purpose of introducing this provision was to endow upon body corporates the responsibility of protecting data and adopting reasonable security measures to that effect. The provision also imposes on the body corporate the burden to prove that sufficient security measures had been installed in the event a breach of security does indeed take place. With the same objective, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were passed in 2011, and the Central Government simultaneously clarified the concept of 'sensitive personal data' vide a notification. Contextually, the concept of '**Cloud Computing**' becomes relevant, whereby networks of remote servers hosted on the internet instead of local servers are used to store and manage data so as to enable more organizations to deal with data belonging to other subjects stored in systems other than their own.

Section 67 as existent in the Act of 2000 was subsequently broadened by the Amendment Act of 2008 to address child pornography, and powers of intermediaries in publishing or transmitting obscene content across cyberspace in electronic format. The provision goes on to expressly capture that any individual publishing on or transmitting through cyberspace any content that is lascivious and is likely to corrupt those coming across such content, shall be imprisoned for a term of three years in prison and a fine of Rs. 5,00,000/- (Rupees Five Lakhs only) in first conviction and be imprisoned for a term of five years and/or a fine of Rs. 10,00,000 (Rupees Ten Lakhs only) in case of second conviction. In the landmark judgment of State of Tamil Nadu v SuhasKatti which was the first conviction in the country under the Information Technology Act, 2000, involved a significant role being played by section 67 of the Act. Similar to section 67, **section 67A** deals with the transmission or publishing of sexually explicit content across cyberspace and enlists it as another punishable offence. Likewise, **section 67B** addresses child pornography thereby criminalizing the act of depicting children, ie, those under the age of 18 (eighteen) years, in sexually explicit activities or creating and advertising such content, or facilitating child abuse on online platforms. The punishment under section 67B may include a fine of Rs. 10,00,000/- (Rupees Ten Lakhs only) and/or an imprisonment for upto five years. Content created or distributed for the purposes of education are however exempted under this provision. **Section 67C** endows upon all digital platforms acting as intermediaries the responsibility of maintaining necessary records as mandated by the law.

Section 69 of the Act provides to the Central Government the authority intercept, monitor or decrypt information that gets transmitted across cyberspace in accordance with the rules of compliance as established by the law and in the interest of the country. Likewise, **section 69A** allows the Central Government or its officers to block content available across cyberspace in the interest of the country; and **section 69B** deals with the power of authorizing such regulation of data through computer resource. Although it cannot be denied that this provision has the potential to be extensively intrusive, it has to be acknowledged that the Central Government has invoked the exercise of such provision only at the rarest of rare instances. The Act further releases all intermediaries of their liability in the third-party information hosted in the website of such intermediaries through **section 70**. Simply put, by virtue of this provision, intermediaries shall not be held for the content made available on/transmitted through their platforms by third parties.

The Act further provides for the establishment of quasi-judicial bodies for hearing disputes and adjudicating them by awarding compensation as well as imposing penalties for civil and criminal liabilities respectively. While Cyber Appellate Tribunal acts as the first appellate body, the High Court serves as the second one.

1.5 RELEVANCE

As opposed to the multiple legislations addressing issues of cyber law in other countries, the Information Technology Act of 2000 and the Information Technology Amendment Act of 2008 single-handedly act as the most significant law striving towards establishing a crime-free society in the country. It cannot be denied that the technology is ever growing and hence demands the law to keep pace with it and address all possible instances of cybercrimes. Although the Information Technology Act does not deal with all such probable situations, such as jurisdictional issues in cybercrimes, it covers a fairly substantial area of cyber law and acts evidently as the most significant piece of legislation on the subject.

1.6 INDIAN PENAL CODE – RELEVANCE IN CYBER LAW

The Indian Penal Code of 1860, the most significant piece of legislation on criminal jurisprudence in the country addresses the substantive facets of criminal law. In accordance with the changes in technology and the evolution and establishment of cyber laws brought in with the advent of the Information Technology Act of 2000, it became necessary to amend various sections of the Code in keeping with the new laws established. With the Act of 2000 acknowledging and recognizing electronic records and electronic evidence at the level of same importance as physical records and evidence, the ambit of the Indian Penal Code has been broadened to include electronic records and documents at par with physical records. Following such amendment, all provisions dealing with instances of false entry, or forgery of documents now include references to electronic documents and records. The provisions of the Code which have undergone amendment are as follows –

- Section 463 – Making or possessing counterfeit seal etc. with the intent to commit forgery
- Section 464 – Making a false document
- Section 468 – Forgery for the purpose of cheating
- Section 469 – Forgery for the purpose of harming reputation
- Section 470 – Forged document or electronic record
- Section 471 – Using as genuine a forged document or electronic record
- Section 474 – Having possession of forged document or electronic record knowing it to be a forgery and intending to use it as genuine
- Section 476 – counterfeiting device or marks used for authenticating documents or electronic records other than those mentioned in section 467, or possessing counterfeit marked materials.

1.7 CYBERSPACE AND THE LAW OF EVIDENCE

Electronic evidence is explicitly recognized in India and is addressed statutorily under various provisions of the Indian Evidence Act, 1872. Any electronic evidence may be produced in court though devices such as CDs, hard drives, etc. With the rise in cybercrimes, it cannot be denied that the evidence of such crimes as available in digital media gains utmost significance in the adjudication of matters relating to such crimes. Since digital evidence is invisible to common eye unless captured or stored in any specific mode or medium, thereby digitally capturing such evidence.

Section 3 of the Indian Evidence Act expressly defined that evidence shall include 'electronic records produced for the inspection of the court'. Additionally, **section 17** of the Indian Evidence Act has been amended to include that the definition of 'admission' for the purposes of the Act to include statements in electronic form as well in addition to oral and documentary admission. **Section 65A** and **65B** are to be read in sync with each other, wherein the former lays down that electronic records and their contents are to be established in accordance with section 65B, which stipulates that electronic evidence contained is to be considered admissible even in absence of the proof of the originals being produced, provided however, certain statutory technical mandates are fulfilled. The provision under section 65B is a non-obstante clause, and is hence deemed to override all general provisions on secondary evidence under the Indian Evidence Act.

1.8 THE BANKERS' BOOK EVIDENCE ACT, 1891

Similar to the provisions of the Indian Evidence Act, the Bankers' Books Evidence Act also ensures that electronic evidence produced in devices such as CD, hard drives, etc. are to be considered valid. Furthermore, the definitions clause in the Act was amended to incorporate that that any form of electromagnetic data storage device shall be included in the definition of 'bankers' books' and 'certified copy'. Additionally, a new section has been incorporated in the Act to include conditions that are to be followed while providing a printout of any certified copy, which might include data stored in digital drives or any other electronic medium.

After the enactment, as per Section 2 i.e., the definitions clause of the Bankers' Books Evidence Act was amended as: 'bankers' books include ledgers, day-books, cashbooks, account-books and

all other books used in ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device'. The amendment in the provisions of the act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms mentioned in the act.

1.9 RESERVE BANK OF INDIA ACT, 1934

The Information Technology Act, 2000 by introducing amendment in the Reserve Bank of India Act, 1934 has given it a contemporary dimension. One of the important functions of the banking system is to help the customers transfer funds to pay bills and invoices, ensure timely payment when crossing multiple time zones and fund trade transactions. It requires close coordination among the banks.[111]

In the Reserve Bank of India Act, 1934, in ***Section 58, in sub-section (2), after clause (p),*** the following clause shall be inserted, namely:-

(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in ***clause (c) of Section 45-1,*** including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund "transfers".

The insertion of aforesaid clause (pp) in the act is a step to introduce and regulate electronic fund transfer mechanism between the banks and other financial institutions. The idea is to overcome the ***'paper-trail'*** of payment transactions. The said provision calls for laying down of conditions for interbank participation in fund transfers, manner of such fund transfers and the rights and obligations of the participants in such transfers.

1.10 LET'S SUM UP

[111] AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934 <http://www.cyberlawclinic.org/rbi.htm>

In this unit we have studied the existing laws in the country addressing the disputes and the crimes pertaining to cyberspace. We have seen the relevant provisions along with the various amendments that took place in Indian Penal Code, Indian Evidence Act, The Bankers' book Evidence Act and finally The Reserve Bank of India Act.

1.11 FURTHER READING

- Iibf.org.in (2019), http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf (last visited Nov 16, 2019).
- http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-160
- Acadpubl.eu (2019), https://acadpubl.eu/hub/2018-119-17/2/141.pdf (last visited Nov 16, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the existing laws in the country addressing disputes and crimes related to cyberspace?**

A. The existing laws in the country addressing disputes and crimes related to cyberspace are as follows:

- Information Technology Act in 2000
- Information Technology Amendment Act, 2008
- Provisions in various other existing legislations that were amended owing to the introduction of the Acts of 2000 and 2008.

2. What are the relevant provisions of the Information Technology Act associated with cyberspace?

A. The relevant provisions of the Information Technology Act associated with cyberspace are as follows-

- Section 66 – Computer related offences (including the sub sections to section 66)

- Section 67 – Punishment for publishing or transmitting obscene materials in electronic form (including the sub sections to section 67)

- Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

- Section 70 – Protected System

- Section 43 – Penalty and compensation for damage to computer, computer system etc.

3. What are the relevant provisions of the Indian Penal Code, 1860 associated with cyberspace?

A. The relevant provisions of the Indian Penal Code, 1860 associated with cyberspace are as follows:

- Section 463 – Making or possessing counterfeit seal etc. with the intent to commit forgery

- Section 464 – Making a false document

- Section 468 – Forgery for the purpose of cheating

- Section 469 – Forgery for the purpose of harming reputation

- Section 470 – Forged document or electronic record

- Section 471 – Using as genuine a forged document or electronic record

- Section 474 – Having possession of forged document or electronic record knowing it to be a forgery and intending to use it as genuine

- Section 476 – counterfeiting device or marks used for authenticating documents or electronic records other than those mentioned in section 467, or possessing counterfeit marked materials

4. What are the relevant provisions of the Indian Evidence Act associated with cyberspace?

A. The relevant provisions of the Indian Evidence Act associated with cyberspace are section 3, section 17, section 65A and section 65B.

1.13 ACTIVITY

Explain in detail admissibility of electronic evidence with the help of case laws. (1000 words)

Block 3
Personal Jurisdiction in Cyberspace

Unit 1: Establishment of Personal Jurisdiction in Cyberspace

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 The U.S. Approach to Personal Jurisdiction

1.4 Establishing Personal Jurisdiction

1.5 Establishing Personal Jurisdiction in Cyberspace

1.6 Nature of the website

1.7 Interactive Websites

1.8 Interactive Mixed Websites

1.9 Passive Websites

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The U.S. Approach to Personal Jurisdiction
- Nature of websites
- Interactive and Passive Websites

1.2 INTRODUCTION

E-Commerce is 24/7 commerce. It is an online activity involving the exchange of goods and services for a consideration (money). Such activity may lead to disputes, which could be (a)

municipal (domestic) or (b) international. The question is how to resolve these disputes keeping in view the complexity of the online activity.

The resolution depends on identifying the 3Ws of the online dispute: What, Where and Why. From the point of identifying the jurisdiction, it is important to know the nature of the dispute and for that purpose, the following questions are necessary:

- What has happened?
- Where did it happen? and
- Why did it happen?

The answers would provide not only the necessary information related to the business model of the website but also the extent of commercial interaction between the service provider (website owner) and the user.

The traditional principles of domestic and international jurisdiction that have been developed and adopted over a period of time are now being extended to cyberspace to formulate a new idiom of cyber jurisdiction. This adoption, in a way, would maintain continuity of established law and practice even in the realm of online activities.

1.3 THE U.S. APPROACH TO PERSONAL JURISDICTION

It is important to understand the enactments of the long-arm statute and the due process of law of the U.S. Constitution to know how these principles have been used by various courts to resolve e-commerce related disputes.

The principle ***'long-arm statute'*** authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action (tortious or any other) falls within the nature of activity required to qualify for jurisdiction.

Over a period of time the States of the US have developed their own respective long-arm statute to exercise personal jurisdiction over any non-domiciliary *"who commits a tortious act within the state"* as long as the cause of asserted arises from the tortious act.

The ***'due process of law'*** as given in the fifth and fourteenth amendment of the US constitution limits the powers of the courts to exercise traditional notions of fair play and substantial justice. The Fourteenth Amendment to the US Constitution provides that *"no state shall deprive any person of life, liberty or property without due process of law"*. The idea is to invoke both long-

arm statute and due process of law provisions to allow the court to exercise personal jurisdiction over any non-domiciliary defendant.[112]

Motion to Dismiss for lack of personal jurisdiction over a non-resident defendant.

End User (Plaintiff)	E-Business (Defendant)
To prove:	
The local state "long-arm statute" applies	Defendant to file and argue a motion to dismiss for lack of personal jurisdiction
There is no violation of defendant's due process rights under the Constitution provision(s).	

1.4 ESTABLISHING PERSONAL JURISDICTION

The credit to establish ground rules for establishing personal jurisdiction for the non-resident lies with the US Supreme Court judgment in ***International Shoe Co. vs State of Washington, Office of Unemployment Compensation and Placement et al[113].*** It held that a court's exercise of personal jurisdiction over a non-resident defendant is proper if that defendant has had certain minimum contacts with (the forum state) such that the maintenance of the suit does not offend *'traditional notions of fair play and substantial justice'*.[114]It established three criteria for establishing ***"minimum contacts":***

- The defendant must *"purposeful avail"* himself of the privilege of doing business with the forum state.
- The cause of action arises from the defendant's activities in the forum state, and
- The exercise of jurisdiction would be fair and reasonable.

The *'minimum contact'* principle laid the foundation of the state's jurisdiction over other state's subject. It advocated the establishment of minimum contacts to give rise to obligations between

[112]Bensusan Restaurant Corp v King - H2O Classroom Tools <https://h2o.law.harvard.edu/cases/4341>

[113]*International Shoe Co. vs State of Washington, Office of Unemployment Compensation and Placement et al* 326 US 310 [316] [1945]

[114]Sykes, Phillip, and Laura McCarthy "Are You Defending Your Clients Where They Don't Belong? Corporate Defendants' New Potent Defense Is Personal (Jurisdiction, That Is)" Defense Counsel Journal, vol 82, no 3, International Association of Defense Counsel, July 2015, p 282

the defendant and the forum state. Primarily, it does not look into the issue whether the contacts were sufficient or insufficient to establish *'purposeful availment'*.

The ***International Shoe Company case*** was decided in the year 1945, and at that time, there were no state long-arm statutes. The long-arm statute went a step ahead of minimum contacts to look into whether the contacts were sufficient to establish purposeful availment like

- Purposefully and successfully solicitation of business from forum (state) residents.
- Establishment of the contract with the forum (state) residents.
- Associated with other forum (state) related activity
- Substantial enough connection with the forum (state)

Once the court determined that sufficient minimum contacts existed to exercise specific jurisdiction over the defendant, the court then would have to consider whether it was reasonable to subject the non-resident defendant to the personal jurisdiction of the forum to the extent that federal constitutional requirements of due process will allow.

The importance of the *International Shoe Company case* is that it established for the first time that personal jurisdiction might exist even though the defendant had no physical presence in the forum state. It acted as a precursor to the states' long-arm statutes. Later, with the advent of e-commerce, this judgment has been used by the courts all over the United States as an established law in identifying minimum contacts to claim personal jurisdiction over a non-resident.

In a nutshell, a state court may acquire valid, specific personal jurisdiction over a non-resident defendant only if:

a) The state's long-arm statute provides for jurisdiction under the factual circumstances and
b) The defendant has had sufficient minimum contacts with the state such that the exercise of jurisdiction does not offend *'traditional notions of fair play and substantial justice'*, violating the due process clause of the 14th amendment.[115]

1.5 ESTABLISHING PERSONAL JURISDICTION IN CYBERSPACE

[115] *KAHN v MAICO COMPANY* 216 F.2d 233 [1954] <https://www.leagle.com/decision/1954449216f2d2331376>

The courts have been borrowing the principles of personal jurisdiction and extending them to the cyberspace setting. The principles of jurisdiction, which were earlier applied to physical establishments, are now being successfully applied to online business establishments (websites).
A website represents a virtual business model. In order to fix the place of jurisdiction, one may have to look into the nature of the websites model – whether it is ***'business-oriented'*** or ***'information-oriented'.*** Other key elements that have to be taken into consideration are: geographical location of users, websites owner and the web server. Even the terms of service agreements, disclaimers and choice of law or forum clauses play an important role.

1.6 NATURE OF THE WEBSITE

An online form of business may exist either in the form of ***(a) Passive website or (b) Interactive website.*** As the name suggest, *'passive'* website is meant for information purposes only, whereas an *'interactive'* website is a dynamic website and provides more than mere information.

Passive Website	Interactive Website
Provides only information	Provides information and facilitates purchasing decisions
Does not solicit business	Purposefully solicits business
Not a revenue model per se	Represents a revenue model
Personal Jurisdiction does not exist	Personal Jurisdiction may or may not exist depending upon fulfillment of the minimum contacts test

Application of minimum contacts and the long arm of statute principles have been used by the courts to determine personal jurisdiction by differentiating between *passive* and *interactive* websites. An important element of minimum contacts is that the contacts need to be of such a character and degree that a defendant could reasonable have expected to be hauled into court in the distant state.

1.7 INTERACTIVE WEBSITES

In ***Cody vs Ward***[116]**,** a Connecticut resident brought suit in Connecticut against a California resident, claiming reliance on fraudulent representatives made by the defendant resulting in a loss.

The court held that it had valid jurisdiction over the defendant based solely upon bulletin board messages posted by the defendant on an online service's ***"Money Talk"*** bulletin board and e-mail messages and telephone conversations from the defendant in California to the plaintiff in Connecticut. It simply concluded that the ***purposeful availment***requirement was satisfied by the defendant's electronic contacts with the plaintiff.

Further in ***CompuServe, Inc. vs Patterson***[117]**,** CompuServe, an Ohio corporation with its main offices and facilities in Ohio, sued one of its commercial shareware providers, a resident of Texas. The suit was filed in Ohio, and the defendant asserted that the Federal District Court in Ohio lacked jurisdiction over him, claiming never to have set foot in Ohio.

The appellate court measured the defendant's ***'contacts'*** with Ohio and concluded that jurisdiction was proper because: **(a)** the defendant has purposefully availed himself of the privilege of doing business in Ohio by subscribing to CompuServe and subsequently accepting online CompuServe's Shareware Registration Agreement (which contained an Ohio choice of law provision) in connection with his sale of shareware programs in the service, as well as by repeatedly uploading shareware programs to CompuServe's computers and using CompuServe's e-mail system to correspond with CompuServe regarding the subject matter of the lawsuit; **(b)** the cause of action arose from Patterson's ***'activities'*** in Ohio because he only marketed his shareware through CompuServe; and **(c)** it was not unreasonable to require Patterson to defend himself in Ohio because by purposefully employing CompuServe to market his products, and accepting online the Shareware Registration Agreement, he should have reasonable expected disputes with CompuServe to yield lawsuits in Ohio.

Similarly, in ***EDIAS Software International vs BASIS International, Ltd.,***[118]where an Arizona based software distributor brought suit in Arizona against a New Mexico software development company arising out of the termination of an agreement between the companies and public statements made by the defendant about the termination. The defendant had no offices in Arizona.

---

[116]*Cody v Ward* 954 F Supp 43 D Conn [1997]

[117]*CompuServe, Inc v Patterson* 89 F 3d 1257 6th Cir [1996]

[118]*EDIAS Software International vs BASIS International, Ltd* 947 F Supp 413 [1996]

The defendant's contacts with Arizona analyzed under the purposeful availment test consisted of: **(a)** a contract with the plaintiff (executed in New Mexico with a New Mexico choice of law provision); **(b)** phone, fax and e-mail communications with plaintiff in Arizona; and **(c)** sales of software products to the plaintiff and other Arizona residents; and visits to Arizona by officers of the defendant. The court upheld the plaintiff's claim of personal jurisdiction over the defendant.
If one analyses the aforesaid three cases, then one may conclude that all the three cases fall in the category of an interactive website, though their degree of interactivity differ:

Minimum **Level of Personal Interactivity** **Maximum**

Cody vs Ward < CompuServe, Incvs Patterson < EDIAS Software International vs BASIS International, Ltd.

In ***Cody vs Ward,*** the level of personal interactivity has been limited to posting of bulletin board messaged and telephonic conversation from the defendant based in California to the plaintiff based in Connecticut, where in ***CompuServe, Inc. vs Patterson,*** the relationship though online, was of a commercial nature. In ***EDIAS Software International vs BASIS International, LTD.,*** the online interaction has been further supported by offline activities, like sale of the goods and visits to Arizona by officers of the defendant.

1.8 INTERACTIVE 'MIXED' WEBSITES

Now supposing that if a company maintains a website for the purpose of soliciting business, then would it be called an interactive website. In ***Maritz, Inc. vsCybergold, Inc.***[119]the court looked at the very basic issue of maintaining a website by the company by framing the due process issue as whether ***"maintaining a website which can be accessed by any internet user, and which appears to be maintained for the purpose of, and in anticipation of being accessed and used by any and all internet users, including those residing in Missouri (accessed 131 times by residents of the forum state), amounts to promotional activities or active solicitations such as***

[119]*Maritz, Inc. vCybergold, Inc*947 F Supp 1328 E D Mo [1996]

to provide the minimum contacts necessary for exercising personal jurisdiction over a non-resident".[120]

The court concluded that because the maintenance of a website is a more efficient and faster means of reaching a global audience, and through its website, CyberGold has consciously decided to transmit advertising information to all internet users, knowing that such information will be transmitted globally. Thus, CyberGold's contacts are of such quality and nature, albeit a very new quality and nature for personal jurisdiction jurisprudence, that they favor the exercise of personal jurisdiction over the defendant.

The court reasoned that setting up a website is a stronger basis for jurisdiction than maintaining a telephone number or a mailing address, since **(i)** a company's establishment of a telephone number, such as an 800 number, is not as efficient, quick, or easy way to reach the global audience that the internet has the capability of reaching, and **(ii)** if a forum resident sends a letter to defendant, (defendant) would have the option as to whether to mail information to the (forum) resident, (whereas defendant) automatically and indiscriminately responds to each and every internet user who accesses its website.

In other words, specially maintaining a website for soliciting business i.e., advertising and promoting the offline activities in an online medium, exemplifies the fact that the website is an interactive one, though of a lesser degree.

Does this mean that maintaining a website for information purpose only would fall in the interactive category?

1.9 PASSIVE WEBSITES

In ***Bensusan Restaurant Corp. vs King,***[121]where a New York jazz club operator sued a Missouri club owner claiming trademark infringement, dilution and unfair competition over the use of the name ***"The Blue Note".*** The defendant maintained a website promoting his Missouri *Blue Note* club and providing a Missouri telephone number through which tickets to the club could be purchased.[122]

[120]*Maritz, Inc v Cybergold, Inc,* 947 F Supp. 1328 <https://law.justia.com/cases/federal/district-courts/FSupp/947/1328/1453704/>

[121]*Bensusan Restaurant Corp v King* 937 F Supp 295 SDNY, [1996]

[122]Cyber Law Cases &Judgements - Advocate Prashant Mali

The issue, as framed by the Federal District Court, was whether the existence of the website, without more, was sufficient to vest the court with personal jurisdiction over the defendant under New York's long-arm statute.

The Court held that it did not. The court considered whether the existence of the website and telephone ordering information constituted an ***offer to sell*** the allegedly infringing product in New York, and concluded it was not. The court noted that, although the website is available to any New Yorker with Internet access, it takes several affirmative steps to obtain access to this particular site, to utilize the information contained there, and to obtain a ticket to the defendant's club.

These steps would include the need to place a telephone call to Missouri and to physically travel to Missouri to pick up the tickets ordered. Therefore, the court concluded that any infringement that might occur would be in Missouri, not New York. The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York.

It found that the defendant did nothing to purposefully avail himself of the benefits of New York. There was no evidence of the defendant actively encouraging New Yorkers to visit the site.

The nature of a website – whether interactive, mixed or passive depends on the business model the said website is subscribing. It is the degree of interactivity that separates an interactive website from the passive one. The level of interactivity has to take into consideration the purposeful availment of the benefits of the forum state in the form of conducting business online and/or offline.

1.10 LET'S SUM UP

In this chapter, we have studied the U.S. Approach to personal jurisdiction along with the jurisdiction in cyberspace. We also studied the nature of the website and finally, we ended the discussion with the interactive websites and passive websites.

1.11 FURTHER READING

<http://www.prashantmali.com/cyber-law-cases>

- Cyber law – Text and Cases, (Ferrera, G.R., Lichtenstein, D.S., Reder, M.E.K., August, R., Schiano, W.T.), West Thomson Learning, USA, 2000, p.21.
- See Jean Gleason & Robert Rosenblum, Current Developments in Regulation D and Rule 144A: The SEC's Efforts to Increase the Effectiveness and Liquidity of the U.S. Private Placement Market, C540 ALI-ABA 443, 449 (1990).
- Jiménez, William and Lodder, Arno R., Analyzing Approaches to Internet Jurisdiction Based on Model of Harbors and the High Seas (August 13, 2015). International Review of Law, Computers & Technology, Vol. 29, No. 2/3, July 2015, p. 266-282.
- See generally Joseph Kalo, Jurisdiction as an Evolutionary Process: The Development of Quasi In Rem and In Personam Principles, 1978 DUKE L. J. 1147 (tracing relationship between jurisdictional evolution and economic development).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the long-arm statute?

The principle ***'long-arm statute'*** authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action (tortious or any other) falls within the nature of activity required to qualify for jurisdiction.

2) What is due process of law?

The ***'due process of law'*** as given in the fifth and fourteenth amendment of the US constitution limits the powers of the courts to exercise traditional notions of fair play and substantial justice. The Fourteenth Amendment to the US Constitution provides that *"no state shall deprive any person of life, liberty or property without due process of law"*. The idea is to invoke both long-arm statute and due process of law provisions to allow the court to exercise personal jurisdiction over any non-domiciliary defendant.

3) Differentiate between Passive and Interactive Website?

Passive Website	Interactive Website
Provides only information	Provides information and facilitates purchasing decisions

Does not solicit business	Purposefully solicits business
Not a revenue model per se	Represents a revenue model
Personal Jurisdiction does not exist	Personal Jurisdiction may or may not exist depending upon fulfillment of the minimum contacts test

1.13 ACTIVITY

Explain the personal jurisdiction in cyberspace along with different types of websites and case laws pertaining to it? (1000 words)

Unit 2: Overview of Tests and Interactivity

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Sliding Scale Approach

1.3 The Limit of Interactivity Criterion

1.4 Interactivity: Online + Offline

1.5 Forum State Targeting

1.6 The Effects Test and Online Interaction

1.7 Conclusion

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Sliding Scale Approach
- Forum State Targeting
- The Effects test

1.2 SLIDING SCALE APPROACH

In ***Zippo Manufacturing Company vs Zippo Dot Com, Inc.,***[123] Zippo Manufacturing Company, a Pennsylvania based corporation has been well known among other things for ***'Zippo'*** tobacco lighters. Zippo Dot Com, Inc. California corporation has been providing free news services

[123] *Zippo Manufacturing Company v Zippo Dot Com, Inc*952 F Supp 1119 W D Pa[1997]

through its website. In addition, the defendant also provided a fee-based service to permit the subscriber to view and/or download Internet newsgroup messages that are stored on the defendant's server in California. The defendant, a California corporation, was sued in Pennsylvania.

Dot Com maintained no offices, employees or agents in the state of Pennsylvania. It has been posting information about its service on its web pages, which are accessible to Pennsylvania residents via the Internet. The defendant had 140,000 paying customers worldwide and out of which around 2%, i.e., 3,000 were Pennsylvania residents. In addition, it had contracted with several Internet access providers in Pennsylvania to permit the Pennsylvania subscribers to access the Dot Com's new service.

Court task was to determine whether Dot Com's conducting of e-commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania. Dot Com not only chose to process Pennsylvania residents' applications but also assigned them passwords.

The Dot Com argued that its forum-related activities were not numerous or significant enough to create a ***'substantial connection'*** with Pennsylvania. It pointed out to the fact that only 2% of its subscribers were Pennsylvania residents.

The court concluded that this level of contact with the state justified the exercise of specific personal jurisdiction. In doing so, however, it reviewed the growing number of cases in the *genre* and tried to provide some synthesis of the varying approaches. The court noted that the cases reveal a ***'sliding scale',*** in which, At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. (***e.g. Compuservevs Patterson)***. At the opposite end are situations where a defendant has simply posted information on an Internet Website, which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction ***(e.g. Bensusan Restaurant Corp., vs King).*** The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and (the)

commercial nature of the exchange of information that occurs on the website. ***(e.g. Maritz, Inc. vsCybergold, Inc.).***

Nature of website	Personal Jurisdiction
Interactive	(+)
Mixed	(+) or (-)
Passive	(-)

To sum up, the sliding scale approach classifies the websites on the basis of interactivity. In ***Bensusan,*** the court refused to exercise jurisdiction based on the website alone, reasoning that it did not rise to the level of purposeful availment of that jurisdiction's laws whereas in ***CompuServe*** the user had *'reached out'* from Texas to Ohio and originated and maintained contacts with Ohio.

These judgments have underlined the fact that personal jurisdiction must adapt to progress in technology and that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportional to the nature and quality of commercial activity that a business entity conducts over the Internet.

1.3 THE LIMIT OF INTERACTIVITY CRITERION

Over a period of time (especially post 1997), the courts have moved away in some cases from the sliding-scale prognosis that personal jurisdiction is directly proportional to the nature and quality of commercial activity that a business entity conducts over the Internet. For example, in ***CyberSell Inc. vsCyberSell Inc.***[124] the court endorsed the sliding-scale set forth in ***Zippo,*** held that mere operation of a website is insufficient to support personal jurisdiction: something more is required to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial wat to the forum state. It concluded, on the facts of this case, that something else was lacking and declined personal jurisdiction over the defendant.

[124] *CyberSellInc vCyberSellInc*130 F 3d [414] 9th Cir [1997]

Similarly, the courts from the other states have not been willing to accept that interactivity of a website alone constitutes ***'purposeful availment'*** of the forum state. Cases in which interactive features of a website were found insufficient to support jurisdiction include: ***3D Systems, Inc. vsAarotech Laboratories, Inc.,***[125] (defendant operated a website describing its subsidiary's products, and received e-mail inquiries via that site, but merely forwarded them to its subsidiary for response); ***American Information Corp. vs American Infometrics, Inc.,***[126] (prospective employees could submit their resumes via the website); ***Ecotecture, inc.vsWenz,***[127] (website allowed visitors to subscribe to an online journal); ***People Solutions, Inc. vs People Solutions, Inc.,***[128] (website contains interactive pages that allow customers to test Defendant's products, download product demos, obtain product brochures and information, and order products online); ***JB Oxford Holdings Inc. vs Net Trade, Inc.,***[129] (visitors could apply for a securities trading account online); ***Desktop Technologies Inc. vsColorworks Reproduction & Design, Inc.,***[130] (site allowed exchange of files via FTP and e-mail); ***Agar Corp. vs Multi-Fluid, Inc.,***[131] (site included links allowing visitors to provide feedback and register).

It seems that the courts have started appreciating and analyzing the website in a holistic fashion rather than in a piecemeal manner. To them, interactivity is not the only criteria for proclaiming personal jurisdiction. Similarly, the features on the website, like a toll-free number and/or link to send an email do not make such website interactive. For example, in ***Osteotech, Inc. vsGenSci Regeneration Sciences, Inc.,***[132] (placement of defendant's phone number or e-mail address on its website is not relevant to the jurisdictional analysis since inclusion of this information has no more of an impact on any particular forum than a website without such information); ***Edberg vsNeogen Corp.,***[133] (no jurisdiction, where site included both a toll-free number and a link for sending e-mail to the defendant); ***Grutkowskivs Steamboat Lake Guides & Outfitters, Inc.,***[134] (inclusion of an e-mail link and local telephone number does not make site interactive); ***Conseco,***

[125] *Systems, Inc vAarotech Laboratories, Inc* 160 F 3d 1373 Fed Cir[1998]
[126] *American Information Corp v American Infometrics, Inc* 139 F Supp 2d 3696 D Md[2001]
[127] *Ecotecture, inc vWenz*[2000] WL 760961
[128] *People Solutions, IncvPeople Solutions, Inc*[2000] WL 1030619 N DTex [2000]
[129] *JB Oxford Holdings Inc v Net Trade, Inc* 76 FSupp 2d 1363 S D Fla [1999]
[130] *Desktop Technologies Inc vColorworks Reproduction & Design, Inc*[1999] WL 98572 E D Pa[1999]
[131] *Agar Corp v Multi-Fluid, Inc* 45 U S P Q 2d BNA 1444 S DTex [1997]
[132] *Osteotech, Inc vGenSci Regeneration Sciences, Inc* 6 F Supp 2d 349 D N J [1998]
[133] *Edberg vNeogen Corp* 17 F Supp 2d 104 D Conn [1998]
[134] *Grutkowski v Steamboat Lake Guides & Outfitters, Inc*[1998] WL 962042 E D Pa [1998]

Inc. vsHickerson,[135] (no jurisdiction, where site included e-mail link); ***Transcraft Corp. vsDoonam Trailer Corp.,***[136] (no jurisdiction, where site includes a toll-free number and invites inquires by e-mail).

1.4 INTERACTIVITY: ONLINE + OFFLINE

As discussed previously, on the scale of interactivity, the 'plaintiff-defendant' interaction in ***EDIAS Software International vs BASIS International, Ltd.,***[137]has been identified as the highest (maximum) since the online interaction between them has been further supported by offline activities, like sale of the goods and visits to Arizona by officers of the defendant.

Increasingly, courts have been going beyond the online interaction and looking at whether there has been some ***'additional contacts'*** to satisfy due process requirements for jurisdiction. For example, in ***Starmedia Network, Inc. vsStarMedia Ins.,***[138]the defendant's website allowed visitors to register, download dealer applications, obtain password-protected product and pricing information. The criteria, but found that its interactivity was limited. It held, however, that the due process requirements for jurisdiction were satisfied in view of additional contacts that defendant had with the forum state. Similarly, in ***Hsin Ten Enterprise USA, Inc. vs Clark Enterprises,***[139] the court did not ground jurisdiction on defendant's interactive website alone, but noted that defendant sent representatives to attend trade shows in the forum state, maintained independent affiliates there, and had sold its products to residents of the forum state.

Hence, it is important to note that the meaning of website interactivity does no longer imply online interaction only. The courts have been looking into some additional offline contacts for proper application of personal jurisdiction.

1.5 FORUM STATE TARGETING

Another trend that has been emerging is that the courts are now increasingly taking cognizance of the commercial involvement of the residents of the forum state. The earlier concept of

[135] *Conseco, Inc vHickerson*698 N.E.2d 816 Ind App [1998]
[136] *Transcraft Corp vDoonam Trailer Corp*45 U S P Q 2d (BNA) 1097 N D Ill [1997]
[137] *EDIAS Software International v BASIS International, Ltd*947 F Supp 413 D Ariz[1996]
[138] *Starmedia Network, Inc vStarMedia Ins*[2001] WL 417118 (SDNY 2001)
[139] *Hsin Ten Enterprise USA, Inc v Clark Enterprises*138 FSupp 2d 449 SDNY [2000]

'general interaction' has given way to ***'specific interaction'*** for the purpose of invoking special personal jurisdiction. For example, In ***Millennium Enterprises Inc. vs Millennium Music, LP,***[140] the plaintiff which operated music stores in Oregon under the name *'Music Millennium,'* claimed that defendant violated its trademark in that name by operating in South Carolina under the name *'Millennium Music'*. Defendant's website allowed visitors to purchase compact disks, join a discount club, and request franchising information, but no residents of Oregon had made any purchases via the website or engaged in any online communication with the defendant. The court rejected the view that potential interactivity is sufficient to satisfy due process. It held that there must, in addition, be some *'deliberate action'* with the forum state, consisting of either transactions with residents of the forum state or other conduct purposefully directed at them. The court opined, 'Until transactions with Oregon residents are consummated through defendants' Website, defendants cannot reasonably anticipate that they will be brought before this court'.

Also, in ***Quokka Sports, Inc. vs Cup Int'l Ltd.,*** [141] the defendants, a company and individuals based in New Zealand, operated websites under domain names that allegedly infringed plaintiff's trademarks. The court found that the content of the website reflected the defendants' intention to target the U.S. market. In reaching that result, the court relied on the facts that **(1)** defendants purposefully went to the United states registrar, NSI, to gen ***'.com'*** domain name, rather than staying at home and registering a ***'county-specific .nz'*** domain; **(2)** the website featured banner advertisements from ten U.S. companies; some of the ads, when clicked, displayed a page designed for U.S. Consumers; **(3)** defendants quoted advertising rates to prospective advertisers in U.S. dollars; **(4)** the website offered to sell travel packages that were priced in U.S. dollars; and **(5)** the website offered books for sale, in affiliation with Amazon.com, a U.S. company.

Both the aforesaid cases point out that the targeting of the forum state is an important criterion in establishing personal jurisdiction.

1.6 THE EFFECTS TEST AND ONLINE INTERACTION

[140] *Millennium Enterprises Inc v Millennium Music, LP* 33 F Supp 2d 907 (D Or)[1999]
[141] *Quokka Sports, Inc v Cup Int'l Ltd* 99 FSupp 2d 1105 (ND Cal)[1999]

Another criterion that has been accepted by the courts has been the ***"Effects"*** of online interaction on the forum state. The US Supreme Court in ***Calder vsJones,***[142] held that the minimum contacts due process requirement may be satisfied on the basis of the effects that out-of-state conduct has in the forum state. In that case, the Court held that a California court could assert jurisdiction over a Florida publisher that published an article defaming the plaintiff, in view of the facts that plaintiff resided in California. The Court reasoned that the defendants had engaged in *'international, and allegedly tortious, actions (that were) expressly aimed at California,'* and that they knew that the brunt of the injury would be felt by the plaintiff in California.

The effect test is a further extension of the forum state targeting, as it also takes into consideration the effect that out-of-state conduct has in the forum state. Thus, in order to have personal jurisdiction, there must be: **(1)** intentional actions **(2)** expressly aimed at the forum state **(3)** causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.[143]

What separates the effect test from other personal jurisdiction approaches is that the focus is on the ***knowledge*** or ***likelihood*** of causing harm in the forum state. All the previous approaches put more focus on the level of either online or online as well as offline interactions. That's why more and more cases involving defamation or infringement of intellectual property rights have been decided on the basis of this test. For example, in ***Telco Communications vs An Apple a Day,***[144] (The Virginia plaintiff sued the Missouri defendant for, inter alia, defamation in Internet press releases from which the plaintiff's stock prices suffered. The court held the exercise of jurisdiction to comport with due process since the defendant knew the statements would be damaging to the plaintiff and was aware of the location of the plaintiff in Virginia); ***PurCo Fleet Services, Inc. vs Towers,***[145] (defendant registered domain name corresponding to plaintiff's trademark, and set up website that forwarded visitors to its own site); ***3DO Co vsPoptop Software Inc.,***[146] (defendant's website allowed visitors to download software that allegedly

[142] *Calder vs Jones* 456 US 783 [1984]
[143] Full text of "final_paper1_(v1i2)" - archive.org <https://archive.org/stream/Final_paper1_v1i2/final_paper1_(v1i2)_djvu.txt>
[144] *Telco Communications v An Apple a Day* Civ Act No 97-542-A (E D Va) [1997]
[145] *PurCo Fleet Services, Inc v Towers* 38 F Supp 2d 1320 (D Utah)[1999]
[146] *3DO Co vPoptop Software Inc* 49 USPQ 2d (BNA) 1469 (ND Cal)[1998]

infringed plaintiff's copyright and misappropriated plaintiff's trade secrets); ***Bunn-O-Matic Corp vs Bunn Coffee Service, Inc.,***[147](defendant's website included terms that allegedly infringed plaintiff's trademarks); ***Digital Equipment Corp vs AltaVista Technology, Inc.,***[148](the court drew an analogy between trademark infringement that occurs on a website and infringement that arrives in the state via other means of communication like telex, telephone, and mail and held that using the Internet under the circumstances of this case is as much knowingly sending into Massachusetts the allegedly infringing and therefore tortious uses of Digital's trademark as is a telex, mail, or telephonic transmission).

The application of the effect test in the online environment is to establish the tortious liability of the defendant and the long-arm reach of the plaintiff's forum state to have personal jurisdiction over such defendants. Similarly in the ***Banyan Tree Holding (P) Ltd vs A. Murali Krishna Reddy,***[149]the Division Bench of Delhi High Court, it was held that effect test to apply where a forum state is justified in assuming personal jurisdiction over a foreign defendant, plaintiff must plead and show *prima facie* that specific targeting of the forum state by defendant resulted in an injury or harm to the plaintiff in the forum state in which case the forum state, can presume jurisdiction over out of state defendant.

1.7 CONCLUSION

The effect test, like the Zippo test is not free from subjectivity. The issue of jurisdiction is often decided at the threshold of litigation on the pleadings and inferences drawn from the pleadings. The same set of facts that might lead one court to conclude that a defendant intended purposefully to cause an effect within a given jurisdiction might not lead another court to the same conclusion. Targeting to some courts simply connotes an effort specifically to reach a person who resides in the forum, rather than to generate an impact there. To other courts, it may only connote that effects within the forum were foreseeable. In the end, the cases suggest that predictability of outcome is perhaps only marginally greater under the effects test than under the sliding scale test.

[147]*Bunn-O-Matic Corp v Bunn Coffee Service, Inc* 46 USPQ 2d (BNA) 1375 (CD Ill)[1998]
[148]*Digital Equipment Corp v AltaVista Technology, Inc*960 F Supp 456 (D Mass) [1997]
[149]*Banyan Tree Holding (P) Ltd v AMurali Krishna Reddy* Judgment dated 23-11-2008 passed in CS (OS) No. 894/2008

1.8 LET'S SUM UP

In this chapter, we have studied the tests and interaction under cyber law. We discussed the sliding scale approach along with the Interactivity in online as well as offline with a plethora of case laws. We also discussed the effects test and online interaction with respect to it. Finally, we ended the discussion with a comparison between effects test, sliding scale test and forum state targeting and the courts view on it.

1.9 FURTHER READING

- Geist,M. (2001).Is There a There There: Towards Greater Certainty in Internet Jurisdiction, 16 Berkeley Tech.L.J. 1345.
- Rice, D. (2002). Refining the Zippo Test: New Trends on Personal Jurisdiction for Internet Activities. The Computer & Internet Lawyer. Prentice Hall Law& Business.
- Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., &Schiano, W. (2003). CyberLaw: Text and cases (2nd ed.). South-Western College/West. ISBN-10: 0324164882, ISBN-13: 978-0324164886.
- Adeika, John. (2015). Cyberlaw - Standard and Legal Issues.10.13140/RG.2.1.3800.5605.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of Sliding Scale Approach?

The sliding scale approach classifies the websites on the basis of interactivity.

2) What is the Effect Test?

The effect test is a further extension of the forum state targeting, as it also takes into consideration the effect that out-of-state conduct has in the forum state. Thus, in order to have personal jurisdiction, there must be: **(1)** intentional actions **(2)** expressly aimed at the forum state

(3) causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.

3) Describe the case Millennium Enterprises Inc. vs Millennium Music, LP?

In ***Millennium Enterprises Inc. vs Millennium Music, LP,*** the plaintiff which operated music stores in Oregon under the name *'Music Millennium,'* claimed that defendant violated its trademark in that name by operating in South Carolina under the name *'Millennium Music'*. Defendant's website allowed visitors to purchase compact disks, join a discount club, and request franchising information, but no residents of Oregon had made any purchases via the website or engaged in any online communication with the defendant. The court rejected the view that potential interactivity is sufficient to satisfy due process. It held that there must, in addition, be some *'deliberate action'* with the forum state, consisting of either transaction with residents of the forum state or other conduct purposefully directed at them. The court opined, 'Until transactions with Oregon residents are consummated through defendants' Website, defendants cannot reasonably anticipate that they will be brought before this court'.

1.11 ACTIVITY

Differentiate between sliding scale approach, Forum State Targeting and the Effects Test with relevant case laws? (1000-1500 words)

Unit 3: Jurisdictional Approaches of Online Contract

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Jurisdiction on the Basis of Online Contract

1.3 Forum Selection Clauses: Click-wrap contracts

1.4 Jurisdiction based on Location of a Web Server

1.5 European Approach to Personal Jurisdiction

1.6 The Brussels Regulation

1.7 Applicability of Brussels Regulation in Online Environment

1.8 Rome Convention

1.9 Applicability of the Rome Convention in Online Environment

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- European approach to personal jurisdiction
- The Brussels Convention
- Rome Convention

1.2 JURISDICTION ON THE BASIS OF ONLINE CONTRACT

Online contracts come with terms of service agreements and disclaimers. These agreements impose restrictions on the users' regarding the choice of law and forum selection. The judicial

view as arrived in ***Bremen vs Zapata Off-Shore Co.,***[150] is that such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be *'unreasonable'* under the circumstances. This rule applies, under the federal law, both if the clause was a result of negotiation between two business entities, and if it is contained in a form of contract that a business presents to an individual on a take-it-or-leave-it-basis.

1.3 FORUM SELECTION CLAUSES: CLICK-WRAP CONTRACTS

It makes a good legal sense for the online service providers to limit their exposure to one jurisdiction only. Defending lawsuits at multiple locations could be both expensive and frustrating. Thus the online service provider has no other choice but to subject themselves to only one set of the forum and applicable laws only. The user has no other choice, but to accept the service provider's terms of service conditions by clicking an on-screen button that says **"I Agree", "I Accept" or "Yes".**

In ***Groff vs America Online, Inc.,***[151] the plaintiff, an individual in Rhode Island who subscribed to America Online, sued the company in Rhode Island state court, alleging violations of state consumer protection legislation. The process of becoming a member of AOL includes a step in which the applicant must assent to AOL's Terms of Service by clicking on ***"I Agree"*** button. The Terms of Service contains a forum-selection clause which expressly provides that Virginia law and Virginia courts are the appropriate law and forum for the litigation between members and AOL. AOL moved to dismiss this suit from the Rhode Island Superior Court for the improper venue on the ground that a forum selection clause in the parties' contract mandated that the suit be brought in Virginia, where AOL's base of operations was located. The court agreed and dismissed the suit.[152]

The court held that the plaintiff assented to AOL's terms of service online by the click of an "I agree" button. The terms of service included a clause mandating that suits concerning the service be brought in Virginia. AOL customers must first click on an "I agree" button indicating assent to be bound by AOL's terms of service before they can use the service. This button first appears

[150] *Bremen v Zapata Off-Shore Co*407 US 1 (9-10) [1972]
[151] *Groff v America Online, Inc*[1998] WL 307001 (R I Super Ct 1998)
[152] The Origin of Click-Wrap: Software Shrink-Wrap Agreements <https://www.wilmerhale.com/en/insights/publications/the-origin-of-click-wrap-software-shrink-wrap-agreements-march-22-2000>

on a webpage in which the user is offered a choice either to read, or simply agree to be bound by, AOL's terms of service. It also appears at the foot of the terms of service, where the user is offered the choice of clicking either an "I agree" or "I disagree" button, by which he accepts or rejects the terms of service. The court held that a valid contract existed, even if the plaintiff did not known of the forum selection clause:

"Our court stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively signed the agreement by clicking "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."

Citing ***Bremen vs Zapata,*** the court looked to whether enforcement of the clause would be unreasonable. It did so by application of a nine-factor test, including such criteria as the place of execution of the contract, the public policy of the forum state, location of the parties and witnesses, relative bargaining power of the parties, and the conduct of the parties. The court concluded that enforcement of the clause would not be unreasonable, and so dismissed the case.

Similarly in ***Steven J. Caspi, et al vs The Microsoft Network, L.L.C., et al.,***[153] the user could not use Microsoft Network unless she clicked the "I agree" button next to a scrollable window containing the terms of use. Each plaintiff clicked the "I agree" button to use Microsoft Network, indicating their assent to be bound by the terms of the subscriber agreement and thus forming a valid license agreement. The Superior Court of New Jersey held that the forum selection clause contained in Microsoft Network subscriber agreements was enforceable and valid.

It is important to note that in ***Groff vs America Online, Inc.,*** the court had also taken into consideration the "place of execution" of the online contract. It opined, "The place where the transaction has been performed appears to take place where defendant's mainframe is located (Virginia)." and not the place (Rhode Island) when plaintiff clicked the "I Agree" button.

In other words, the courts have also started realizing the location of equipment (computer network) as one of the important elements to assert personal jurisdiction.

[153] *Steven JCaspi, et al v The Microsoft Network, L L C, et al*[1999] WL 462175, 323 NJ Super 118 (NJ App Div, July 2, 1999)

1.4 JURISDICTION BASED ON LOCATION OF A WEB SERVER

Asserting personal jurisdiction based on the defendant's use of IT infrastructure of a service provider, located in the forum state, to host its website may also compel the forum state to exercise its jurisdiction over such defendant.

In ***Jewish Defense Organization, Inc. vs Superior Court,***[154] the plaintiff brought an action for defamation in a California court. Defendants' only relevant contacts with California consisted of contracting with Internet service providers, "located in California," to host a website which they maintained from their residence in New York. The court concluded that the defendant's conduct of contracting, via computer, with Internet service providers, which may be California corporations or which may maintain offices or databases in California, is insufficient to constitute purposeful availment. But in ***3DO Co. vsPoptop Software Inc.,*** the court found it relevant that defendants use a San Francisco-based company as a server to operate a website that distributes allegedly infringing copies of software.

Location of a web server alone cannot be taken as a sufficient cause to constitute purposeful availment. Hosting a website means allotting some space on the webserver. One may have to look into the kind of services provided by the web hosting company and the frequency of their utilization by the web promoter to establish purposeful availment of the forum state where the server is located.

The whole discussion on personal jurisdiction has been able to point out that the courts are beginning to understand the true nature of the website(s). The decisions given by them are more or less based on interpreting the 'revenue' model of the website and the level of interaction it achieved while managing a business transaction. Importantly, the courts have also realized the fact that 'online' business has 'offline' manifestations as well, and it is not prudent to ignore the latter.

Another noticeable feature that has emerged is that 'online' promoter has certain advantages vis-à-vis the user, i.e., in terms of selecting the forum. Location of the webserver has a role to play in deciding the question of personal jurisdiction but again it is the level of interaction between the service provider and the user, which would establish purposeful availment of the forum state.

[154] *Jewish Defense Organization, Inc. v Superior Court*85 Cal Rptr 2d 611 (Cal Ct App)[1999]

1.5 EUROPEAN APPROACH TO PERSONAL JURISDICTION

The European approach to personal jurisdiction in cross-border dispute is rather different from the American approach. The rules determining which country's courts have jurisdiction over a defendant are set out in a regulation issued by the Council of the European Union, known as the Brussels Regulation. This new regulation[155] is an update of a 1968 treaty among European countries, known as the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters.

1.6 THE BRUSSELS REGULATION

The Brussels Regulation, which became effective on March 1, 2002, (the Regulation[156] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the EFTA countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.[157]

1.7 APPLICABILITY OF BRUSSELS REGULATION IN ONLINE ENVIRONMENT

The Brussels Regulation has become the established law to resolve disputes concerning jurisdiction and enforcement of judgments in civil and commercial matters. The Regulation is also applicable to resolve online commercial disputes.

On the issue of jurisdiction the Brussels Convention (remained unchanged in the Regulation), sets the rule: Subject to the provisions of this Convention, persons domiciled in a Contracting State shall, whatever their nationality, be sued in the courts of that State (Article 2). Furthermore, A person domiciled in a Contracting State may, in another Contracting State, be sued: in matters

[155]1990 O J (C 189) 2 (consolidated).
[156]Regulation 9EC) No 44/2001 2001 O J 16 January 2001 L 121.
[157]Brussels Convention on Jurisdiction and the Enforcement <https://www.jus.uio.no/lm/brussels.jurisdiction.and.enforcement.of.judgments.in.civil.and.commercial.matters.convention.1968/doc.html>

relating to the contract, in the courts for the place of performance of the obligation in question (Article 5.1). This means that an individual (including a sole trader or partner in a business sued on his own) can be sued where his principal residence is. Article 60 provides that the domicile of a company or other association (including a partnership) is where it has its statutory seat (i.e., its registered office), its central administration or its principal place of business.

From the point of promotions and sale, the Convention says that the consumer may bring proceedings in his own court against a trader if in the state of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising (Article 13), while the Regulation says that the consumer may sue at home if the trader pursues commercial activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State (Article 15).

As websites are generally accessible from anywhere, thus a trader with a website might said to be directing its activities to all EU countries. In case of a dispute, a consumer has a right under Article 15 to take legal action in his or her home court. Any judgment given there would be enforceable in the trader's own country. Article 15 has broadened the scope of traders' liability, as they can now be sued in foreign courts, i.e., for an online trader defending lawsuits at multiple locations could be both expensive and frustrating.[158]

It would be for the European Court of Justice to decide what constituted directed activities. A website may be seen directed to other states if it offers a choice of the languages or currencies of those states, or gives product specifications or delivery times or prices for them. It amounts to a marketing exercise whereby a website is promoting (or targeting) its products or services to consumers in specific EU states.[159]

1.8 ROME CONVENTION

To resolve such cross border consumer contractual disputes, the EU Member States became signatories to the Rome Convention, 1980. It decides which country's law would apply in

[158] Geist, M (2001).Is There a There There: Towards Greater Certainty in Internet Jurisdiction, 16 Berkeley Tech L J 1345

[159]The UK Department of Trade and Industry (DTI) had proposed a way out, that if the website is directed at a particular foreign territory, then the consumer can bring proceedings against the trader in their home state, but if the website is a general site, and not especially directed at the consumer's territory, then trader's own local law would be applicable.

contractual disputes. The Convention gave freedom of choice to the contracting parties: A contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonable certainty (Article 3.1). It further states that the mandatory rules of the consumer's country of habitual residence will always apply whatever choice of law is made (Article 5).

The Convention further provides that in the absence of choice of law the contract is to be governed by the law of the country with which it is most closely connected (Article 4.1), and it presumes that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has his habitual residence or its central administration (Article 4.2). The performance constitutes the essence of the contract and is generally understood to mean the performance for which the payment is due. It operates by reference to the country where the party who is to affect the characteristic performance has his habitual residence, or, in the case of a company, its central administration.

The Convention contains in Article 5 provisions on consumer contracts, which are similar, though not identical, to those in Article 15 of the Brussels Regulations. It states that: Notwithstanding the provisions of Article 3, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence (Article 5.2):

- If in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all steps necessary on his part for the conclusion of the contract, or
- If the other party or his agent received the consumer's order in that country, or
- If the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer's journey was arranged by the seller for the purpose of inducing the consumer to buy.

It is important to note that the mandatory rules of the law cannot be limited or excluded by contractual agreement. They include the rights given to consumers by national legislations.[160] Therefore if the contract meets one of the tests in Article 5.2, the court will apply the law of the consumer's country in deciding the parties' rights and obligations under the contract, regardless

[160]UK on distance selling (e.g., rights to cooling off periods) and the sale of goods (e.g., the right to receive goods, which are of satisfactory quality

of any choice of law to the contrary. It also provides for non-applicability in case of contracts of carriage and contracts for the supply of services, which are to be supplied outside the consumer's country of residence.

1.9 APPLICABILITY OF THE ROME CONVENTION IN ONLINE ENVIRONMENT

Both the Brussels and the Rome Conventions highlight a consumer-oriented Article(s) stating that the consumer may bring proceedings against the trader in the state of the consumer's domicile/habitual residence, if the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising. The questions are – whether these Article(s) are applicable to an online environment also? and does a website promoted by a trader amount to a specific invitation?

Applying the Conventions in an online setting would require an interpretation of the phrase preceded by a specific invitation addressed to him or by advertising i.e., whether an Internet website constitutes advertising in the state of the consumer's domicile. The answer lies in the nature and form of specific invitation.[161]

As far as applicable law is concerned, the courts within the EU apply the Rome Convention even where the applicable law is that of a third country or the parties are not resident or established in the EU.[162]

1.10 LET'S SUM UP

In this chapter, we have studied the jurisdiction on the basis of the online contract along with the concept of jurisdiction based on the location of a web server. We also discussed the European approach to personal jurisdiction, the Brussels regulation and the Rome Convention. Finally, we ended the discussion with the applicability of the aforementioned conventions in the online environment.

[161] Rice, D (2002). Refining the Zippo Test: New Trends on Personal Jurisdiction for Internet Activities.The Computer & Internet Lawyer. Prentice Hall Law& Business

[162]US has not agreed to the Rome and Brussels Convention

1.11 FURTHER READING

- Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000 and November 22, 2000, No RG:00/0538 (Fr.).
- Thomas Schultz, Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface, 19 EUR. J. INT'L L. 779 (2008).
- C. Douglas Floyd &ShimaBaradaran-Robison, Toward a Unified Test of Personal Jurisdiction in an Era of Widely Diffused Wrongs: The Relevance of Purpose and Effects, 81 IND. L.J. 602, 659 (2006).
- Piltz I. (January 22, 2008). Internet law - European Union's Convention on Cyber Crime (ets no. 185): First International Treaty on Crimes Committed via the Internet. Retrieved from http://www.crime-research.org/news/22.01.2008/3144/

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is forum selection clauses based on clickwrap contracts?

Defending lawsuits at multiple locations could be both expensive and frustrating. Thus the online service provider has no other choice but to subject themselves to only one set of the forum and applicable laws only. The user has no other choice, but to accept the service provider's terms of service conditions by clicking an on-screen button that says **"I Agree", "I Accept" or "Yes".**

2) Explain the European approach of Personal Jurisdiction?

The European approach to personal jurisdiction in cross-border dispute is rather different from the American approach. The rules determining which country's courts have jurisdiction over a defendant are set out in a regulation issued by the Council of the European Union, known as the Brussels Regulation. This new regulation[163] is an update of a 1968 treaty among European

[163]1990 O.J. (C 189) 2 (consolidated).

countries, known as the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters.

3) What is the Brussels Convention?

The Brussels Regulation, which became effective on March 1, 2002, (the Regulation[164] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the EFTA countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.

4) What was the reason behind the enforcement of the Rome Convention?

To resolve such cross border consumer contractual disputes, the EU Member States became signatories to the Rome Convention, 1980. It decides which country's law would apply in contractual disputes. The Convention gave freedom of choice to the contracting parties: A contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonable certainty (Article 3.1).

1.13 ACTIVITY

Explain the European Approach to Personal Jurisdiction along with the Brussels and Rome Convention? Also, elucidate the applicability of both the convention with relevant case laws? (1000 – 1500 words)

[164]Regulation 9EC) No 44/2001 2001 O.J. 16 January 2001 L 121.

Unit 4: Basics of Jurisdiction and Indian Approach

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Indian Approach to Personal Jurisdiction

1.3 Jurisdiction based on Forum of Choice

1.4 Jurisdiction based on Code of Civil Procedure

1.5 Basis of Jurisdiction

1.6 Cause of action and Contractual obligations

1.7 Choice of law

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Jurisdiction based on forum of choice
- Jurisdiction based on CPC
- Cause of action and Contractual obligations

1.2 INDIAN APPROACH TO PERSONAL JURISDICTION

It is within the power of the Indian courts to grant an injunction or anti-suit injunction[165] to a party over whom it has personal jurisdiction, in an appropriate case. This is because of courts of

[165]When a court restraints a party to a suit/proceeding before it from instituting or prosecuting a case in another court including a foreign court, it is called anti-suit injunction.

equity exercise jurisdiction in personam. This power is to be used sparingly as though it is directed against a person, but may cause interference in the exercise of jurisdiction by another court. More so, as the courts have to observe the rule of comity,[166] which states that the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its citizens or of other persons who are under the protection of its law.

Keeping in view the nature of the online commerce involving business-to-business (B2B) or business-to-consumer (B2C) contracts, it is important that the issue of personal jurisdiction should be looked into from all possible sources: **(a)** forum of choice **(b)** civil procedure code, 1908 and **(c)** choice of law.

These sources do not constitute mutually exclusive categories. They are dependent upon each other.

1.3 JURISDICTION BASED ON FORUM OF CHOICE

In fact, the parties may themselves agree beforehand that for resolution of their disputes, they would either approach any of the available courts of natural jurisdiction or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. Thus it is open for a party for his convenience to fix the jurisdiction of any competent court to have their dispute adjudicated by that court alone. In other words, if one or more courts have the jurisdiction to try any suit, it is open for the parties to choose any one of the two competent courts to decide their disputes. In case parties under their agreement expressly agree that their dispute shall be tried by only one of them then the parties can only file the suit in that court alone to which they have so agreed.[167]

The growing global commercial activities gave rise to the practice of parties to a contract agreeing beforehand to approach for resolution of their disputes thereunder either any of the available courts of natural jurisdiction and thereby create an exclusive or non-exclusive

[166] *Hilton vGuyot,* 115 US 113 (163-164) [1995]
[167] *Shriram City Union Finance Corporation Ltd v Rama Mishra,* [2002] 9 SCC 613; [2002] AIR SCW 2617; AIR [2002] SC 2402

jurisdiction in one of the available forums or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. It is the well-settles principle[168] that by agreement the parties cannot confer jurisdiction where none exists, on a court to which CPC applies, but this principle does not apply when the parties agree to submit to the exclusive or non-exclusive jurisdiction of a foreign court. Thus, it is clear that the parties to a contract may agree to have their disputes resolved by a foreign court termed as a neutral court or court of choice creating exclusive or non-exclusive jurisdiction in it.

Significantly, in ***Hakam Singh vs Gammon (India) Ltd.,***[169] the Supreme Court held that where two courts or more have under the Code of Civil Procedure jurisdiction to try a suit or proceeding, an agreement between the parties that the dispute between them shall be tried in one of such courts is not contrary to public policy. Such an agreement does not contravene Section 28 of the Contract Act.

In another significant judgment, the Supreme Court has ruled in ***DhannalalvsKalawativai,***[170] there is no wrong without a remedy ***(Ubi jus ibiremedium).*** Where there is a right, there is a forum for its enforcement. The plaintiff is ***dominuslitis,*** that is, master of, or having dominion over the case. In case of conflict of jurisdiction, the choice ought to lie with the plaintiff to choose the forum best suited to him unless there be the rule of law excluding access to a forum of the plaintiff's choice or permitting recourse to a forum will be opposed to public policy or will be an abuse of the process of law.

It is very much clear from the aforesaid discussion that the forum of choice is discretionary and at the instance of the contractual parties. The parties may submit themselves to the exclusive or non-exclusive jurisdiction of either natural or neutral forum.

1.4 JURISDICTION BASED ON CODE OF CIVIL PROCEDURE

In all civil matter, the Code of Civil Procedure (CPC), 1908, formulates the Indian approach to jurisdiction. Under CPC, one or more courts may have jurisdiction to deal with a subject matter having regard to the location of immovable property, place of residence or work of a defendant

[168] *Modi Entertainment Network v W S G Cricket Pte Ltd,* [2003][4] SCC 341; AIR [2003] SC 1177; [2003] AIR SCW 733
[169] *Hakam Singh v Gammon (India) Ltd*[1971][1] SCC 286; AIR [1971] SC 740; [1971] [2] SCJ 576
[170] *Dhannalal vKalawativai*[2002] 6 SCC 16; [2002] AIR SCW 2873; AIR [2002] SC 2572

or place where the cause of action has arisen. Where only one court has jurisdiction, it is said to have exclusive jurisdiction; where more courts than one have jurisdiction over a subject matter, they are called courts of available or natural jurisdiction.

The jurisdiction of the courts to try all suits of civil nature is very expansive, as is evident from the plain language of section 9 of CPC. This is because of the principle of *Ubi jus ibiremedium*(there is no wrong without a remedy).

1.5 BASIS OF JURISDICTION

To formulate whether the jurisdiction of the courts is exclusive or non-exclusive, in the Internet setting, one must involve the jurisdictional principles as highlighted in the CPC:[171]

a) Pecuniary
b) Subject-matter
c) Territory and
d) Cause of action

Pecuniary jurisdiction limits the power of the court to hear cases up to a pecuniary limit only. As Section 6 provides, nothing herein contained shall operate to give any Court jurisdiction over suits the amount or value of the subject matter of which exceeds the pecuniary limits (if any) of its ordinary jurisdiction.

It is important to note that subject to the pecuniary or other limitations prescribed by any law, and jurisdiction also depends on where subject-matter situate (section 16), where a suit is for compensation for wrong done to the person or movable property (section 19) or where defendants reside or cause of action arises (section 20).

Section 19 of CPC states, where a suit is for compensation for wrong done to the person or movable property, if the wrong was done within the local limits of the jurisdiction of one court and the defendant resides, or carries on business, or personally works for gain, within the local limits of the jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said Courts.

[171] Michaels, Ralf (2016) Jurisdiction, Foundations

Section 20 of CPC states, every suit shall be instituted in a Court within the local limits of whose jurisdiction[172] –

a) The defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain; or
b) Any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid acquiesce in such institution; or
c) The cause of action, wholly or in part arises.

(Explanation) – A corporation shall be deemed to carry on business at its sole or principal office in (India) or, in respect of any cause arising at any place where it has subordinate office, at such place.

On one hand, the Section 19 gives an option to the plaintiff to institute the suit at any of the available courts of natural jurisdiction and thus creating an exclusive jurisdiction in one of the available forums, whereas on the other hand, the principle behind the provision of Clauses (a) and (b) of section 20 is that the suit be instituted at a place where the defendant is able to defend the suit without undue trouble. Also, the essential notion of a business, as contemplated by section 20 is that it is commercial in character. The expression ***'carries on business'*** has a commercial flavour and envisages a commercial enterprise.

In ***Gupta Sanitary Stores vs Union of India,***[173] noticing the gamut of law on the point, AvadhBihariRohtagi, J., as His Lordship then was, speaking for self and for SS. Chadha and G.C. Jain, JJ. of this Court, while interpreting the expression carries on business summed up the legal position in the following terms:

[172]'Suit Can Be File Where Both The Parties Decided The Jurisdiction As Per Contract - Legal News / Law News & Articles - Free Legal Helpline - Legal Tips : Legal India' (*Legal News / Law News & Articles - Free Legal Helpline - Legal Tips : Legal India*, 2020) <https://www.legalindia.com/suit-can-be-file-where-both-the-parties-decided-the-jurisdiction-as-per-contract/>

[173]*Gupta Sanitary Stores v Union of India* AIR [1985] Del 122 (FB)

"I take the test to be this: What is the nature and purpose of the activity in question? If it is commercial, the suit can be filed at the principal place of business or principal office. And also at the place where the cause of action arises wholly or in part.[174]

In most cases where the business is not of a commercial nature the suit must be filed against the government at the place where the cause of action arises wholly or in part. For example, if the contract is entered into at Calcutta, the Courts at Calcutta will have the Jurisdiction.[175]

It is significant to note that the expression 'cause of action' has not been defined in the Civil Procedure Code, 1908. It may be referred to as the facts, which give a person the right to seek judicial relief. In ***Rajasthan High Court Advocates' Association vs Union of India,***[176] the Supreme Court held that the expression 'cause of action' has acquired a judicially settled meaning Compendiously the expression means every fact, which would be necessary for the plaintiff to prove, if traversed, in order to support his right to the judgment of the Court. Every fact, which is necessary to be proved, as distinguished from every piece of evidence, which is necessary to prove each fact, comprises in 'cause of action'. It has to be left to be determined in each case as to where the cause of action arises.

1.6 CAUSE OF ACTION AND CONTRACTUAL OBLIGATIONS

The expression 'cause of action' signifies that bundle of facts, which the petitioner must prove, if traversed, to entitle it to a judgment in its favour by the Court. One can find a better answer to aforesaid plea in relation to 'cause of action' by referring to a decision of the Apex Court in the case of ***Oil & Natural Gas Commission vsUtpal Kumar Basu.***[177]It was a case where the petitioner learnt about tenders being invited for a particular project at Hazira in Gujarat from advertisements appearing in the Times of India in circulation in West Bengal by reading it at Calcutta, submitted its offer from Calcutta, made representations and also sent fax messages from Calcutta and received reply thereto at Calcutta. A writ petition was filed

[174]Also see, *Shri Ram Rattan Bhartia v Food Corporation of India*, [1978] Raj LR 177; ILR [1978][1] Del 308; AIR [1978] Del 183 (FB)
[175]*Nalanda Ceramic and Industries Ltd v N S Choudhury and Co (P) Ltd*, AIR [1977] SC 2142; [1978] Pat LJR [12]
[176]*Rajasthan High Court Advocates' Association v Union of India*[2001][2] SCC 294; AIR [2001] SC 416; [2001] AIR SCW [1]
[177]*Oil & Natural Gas Commission vUtpal Kumar Basu*[1994][4] SCC 711; [1994] AIR SCW 3287; JT [1994] [6] SC 1

before the Calcutta High Court on the plea of part of the cause of action having arisen at Calcutta. In view of the aforesaid facts, holding lack of jurisdiction on the part of Calcutta High Court, which it had assumed bypassing impugned order while allowing the appeal, the Supreme Court laid down in the following terms:

"…..merely because it read the advertisement at Calcutta and submitted the offer from Calcutta and made representations from Calcutta would not, in our opinion, constitute facts forming an integral part of the cause of action. So also the mere fact that it sent fax messages from Calcutta and received a reply thereto at Calcutta would not constitute an integral part of the cause of action…".

Where the cause of action arises from contract, and the parties have not effectively selected the governing substantive law, the relevant criteria in a choice-of-law analysis are **(1)** the place of contracting, (**2)** the place of negotiation of the contract, **(3)** the place of performance, **(4)** the location of the subject matter of the contract, and **(5)** the location of the parties.

1.7 CHOICE OF LAW

Based on its assessment of the contractual obligations involved, a court will apply the choice-of-law rules to determine what law should be applied? The two choices are: either to apply the law of the forum (lexfori), or to apply the law of the site of the transaction, or occurrence that gave rise to the litigation in the first place (lex loci). It is obligatory to note that the modern theory of Conflict of Laws recognizes and, in any event, prefers the jurisdiction of the state, which has the most intimate contact with the issues arising in the case. Ordinarily, jurisdiction must follow upon functional lines.[178]

Where the parties have not expressly or impliedly selected the proper law, the Courts impute an intention by applying the objective test to determine what the parties would have as just and reasonable persons intended as regards the applicable law had they applied their minds to the question. The judge has to determine the proper law for the parties in such circumstances by putting himself in the place of a "reasonable man". He has to determine the intention of

[178]*SurinderKaurSandhu vHarbax Singh Sandhu*, [1984][1] Crimes 928: [1984][3] SCC 698: AIR [1984] SC 1224 (1226)

the parties by asking himself "how a just and reasonable person would have regarded the problem".

For this purpose the place where the contract was made, the form and object of the contract, the place of performance, the place of residence or business of the parties, reference to the Courts have jurisdiction and such other links are examined by the Courts to determine the system of law with which the transaction has its closest and most real connection.

It is very much clear that the courts do have a judicial right to determine the choice of law by identifying the system of law with which the transaction has its closest and most real connection. There is no bar that the law of a foreign country cannot be applied or an Indian party could not be subject to a foreign jurisdiction. The emphasis is on to select proper law.

1.8 LET'S SUM UP

In this chapter, we have studied the Indian approach to personal jurisdiction along with the jurisdiction based on the forum of choice and Code of Civil Procedure. We also discussed the cause of action and contractual obligations and finally, we ended the discussion with the Choice of law.

1.9 FURTHER READING

- Suryajyoti Gupta, "Civil and Criminal Jurisdiction in the Internet", Indian Bar Review, Vol. 29 (2002) p. 45; See also Lotus Case, (1927) PCIJ Ser A
- G.R. Ferrera and D.S. Lichtenstein, Cyber Law –Text and Cases, USA, 2000, p. 21
- Ashish A. Agnis, "Personal Internet Jurisdiction: A Case of Digital Confusion", Journal of Symbiosis Law College, 2004, p. 67; See also L. Edwards, Law and the Internet: Regulating Cyberspace, p. 48.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **How the issue of personal jurisdiction should be looked into by the court of law?**

It is important that the issue of personal jurisdiction should be looked into from all possible sources: **(a)** forum of choice **(b)** civil procedure code, 1908 and **(c)** choice of law.

2) **What are the two choices of law?**

The two choices are: either to apply the law of the forum (lexfori), or to apply the law of the site of the transaction, or occurrence that gave rise to the litigation in the first place (lex loci).

3) **What is the meaning of the expression 'cause of action'?**

The expression 'cause of action' signifies that bundle of facts, which the petitioner must prove, if traversed, to entitle it to a judgment in its favour by the Court.

4) **What is the basis of jurisdiction?**

To formulate whether the jurisdiction of the courts is exclusive or non-exclusive, in the Internet setting, one must involve the jurisdictional principles as highlighted in the CPC:

a) Pecuniary
b) Subject-matter
c) Territory and
d) Cause of action

1.11 ACTIVITY

Elucidate the basis of jurisdiction along with jurisdiction based on forum of choice and code of civil procedure with relevant case laws? (1000 words)

Block 4
Freedom of Expression in Cyberspace

Unit 1: Indian Constitutional and Freedom of Expression

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Reasonable Restrictions

1.4 Freedom of Expression and the Internet

1.5 Freedom of Speech and Expression

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The concept of Reasonable restrictions
- Freedom of expression and the Internet
- Freedom of speech and expression

1.2 INTRODUCTION

The Indian Constitution lays down under Article 19 certain fundamental rights to every citizen. The Art. 19 uses the expression *'freedom'* and mentions the several form and aspects of it, which are secured to individuals, together with the limitations that could be, placed upon them in the general interest of the society.

1.3 REASONABLE RESTRICTIONS

Article 19(1)(a) provides that all the citizens shall have the right to freedom of speech and expression. But it should be read with the sub-Art. (2), which imposes reasonable restrictions imposed by the State relating to **(1)** defamation; **(2)** contempt of court; **(3)** decency or morality; **(4)** security of the State; **(5)** friendly relations with foreign states; **(6)** incitement to an offence; **(7)** public order; **(8)** maintenance of the sovereignty and integrity of India.

Hence a law made in respect of the matters referred to in Art. 19(2) must prima facie be presumed to be constitutionally valid and due weight must be given to the legislative judgment on the questions of reasonableness, though that judgment is subject to judicial review.

According to Seervai, H.M., it is difficult, if not impossible, to read into the words "reasonable restrictions" the test of "clear and present danger"[179] evolved by the US Supreme Court in dealing with the freedom of speech and the press. The difference between the First Amendment of the US Constitution and Art. 19(1)(a) was noted by Douglas J. in ***Kingsley Corporation vs Regents of the University of New York,***[180] in holding that all pre-censorship of cinema films was constitutionally void, he said:

"If we had a provision in our constitution for reasonable regulation of the press such as India has included in here there would be room for argument that censorship in the interest of morality would be permissible".

In other words, the Indian Constitution provides that even freedom of speech must yield to public order, i.e., "liberty with order". It was held by the Supreme Court in ***M.H. Devendrappavs Karnataka State Small Industries Development Corpn:***[181]

"The fundamentals freedoms enumerated under Art. 19 are not necessarily and in all circumstances mutually supportive, although taken together they weave a fabric of free and equal democratic society, e.g., the right to reside and settle in any part of the country can be put in

[179]It is important to note that the test of "clear and present danger" has been rejected by the Supreme Court in *BabulalParate v Maharashtra,* AIR [1961] SC 884: [1961][3] SCR 423: [1961][2] Cr LJ 16
[180]*Kingsley Corporation v Regents of the University of New York*[1959] 360 US 684: [1959][3] L Ed 2d 1522
[181]*M H Devendrappa v Karnataka State Small Industries Development Corpn*[1998][3] SCC 732: AIR [1998] SC 1064: [1998] AIR SCW 850

jeopardy by a vociferous local group freely expressing its view against persons from another part of the country. Freedom of speech of one affects the freedom of movement of another. Some restriction on one's rights may be necessary to protect another's rights in a given situation. The rights must be harmoniously construed so that they are properly promoted with the minimum of such implied and necessary restrictions".

1.4 FREEDOM OF EXPRESSION AND THE INTERNET

Keeping in view the concept of "liberty with order", application of the freedom of expression in the context of the Internet would be a restrictive one. The courts would have to first understand the nature of the Internet medium before selectively applying the reasonable restrictions as set out in Article 19(2).

As it was held in ***K. Narayanan vs State,***[182]that "the freedom of speech and expression guaranteed by Article 19(1)(a) included the freedom to acquire knowledge, to read books and periodicals and read any type of literature, subject only to reasonable restrictions being placed on such rights".

Thus the fundamental right of freedom of speech and expression extends to the Internet medium as well. Every citizen has the freedom to acquire or share knowledge (or information) using the Internet and related resources, subject only to reasonable restrictions. The courts may apply reasonable restrictions in the interest of decency or morality to restrict the publication of information which is obscene in electronic form. For this purpose, the courts may have to invoke reasonable restrictions in the interest of decency or morality in light of sections 67, 67A and 67B of the Information Technology Act, 2000 which deals with publication or transmission of obscene material in electronic form.

Earlier as per the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27Th February, 2003, Indian Computer Emergency Response Team (CERT-In) had been designated as the single authority for issuing of instructions in the context of blocking of websites, as there is no explicit provision in the Information Technology Act for blocking of websites. The aforesaid notification

[182]*K Narayanan v State*AIR [1973] Ker 97 (FB)

was based on the premise that such blocking can be challenged if it amounts to restriction of freedom of speech and expression. However, the websites promoting hate content, slander, or defamation of other, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim the constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.

The question is how far the concept of "balanced flow of information" could be stretched. For example, earlier CERT-In attempted to block Meghalaya secessionist email group (groups.yahoo.com/gro-ups/kynhun), and it led to blocking of entire Yahoo Groups site by the overzealous ISPs, with the result complete blackout of communication among the other legitimate users of the Yahoo Groups.

Interestingly, the Central Government has rescinded the aforesaid notification vise Gazette Notification G.S.R. 410(E) dated 17th May 2010. In other words, CERT-In is no longer empowered to block websites or content. The District Court of Delhi in ***Lacoste S.A. vs Ninety Nine Labels (P) Ltd.,***[183] ***Tommy Hilfiger Licencing LLC vs Ninety Nine Labels (P) Ltd.,***[184] and ***Polo Lauren Company vs Ninety Nine Labels (P) Ltd.,***[185] has opined[186] that the Gazette Notification (Extraordinary) No. G.S.R. 181(E), dated 27th February 2003 has been rescinded vide Gazette Notification G.S.R. 410(E) dated 17th May 2010, hence CERT-In is neither a proper or necessary party to block websites or contents thereof. This raises an interesting question – what would be the remedy if someone is aggrieved by defamatory or obscene content?

ILLUSTRATION

Various Options to Block the Content

The following legal options are available to an aggrieved person:

[183] *Lacoste S A v Ninety Nine Labels (P) Ltd*TM No 310/2013
[184] *Tommy Hilfiger Licencing LLC v Ninety Nine Labels (P) Ltd,*TM No 311/2013
[185] *Polo Lauren Company v Ninety Nine Labels (P) Ltd* TM No 312/2013
[186] Vide order dated 23-7-2014.

1) Approach the Grievances Officer as per procedure laid down the Information Technology (Intermediary Guidelines) Rules 2011 and seek directions related to blocking or removal of such content, or
2) Approach the court and seek directions against intermediaries publishing or hosting such content, or
3) Approach the designated Nodal Officer of Ministries or Departments of Government of India or State Governments or any agency of the Central Government with a request that content falling under the provisions of section 69A need to be blocked for public access; Such officer is then to request the Group Coordinator, Cyberlaw Division, Ministry of Communications & Information Technology as per the procedure laid down under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

It is important to note that any censorship is a temporary step, as the 'blocked content' could easily be accessed as cached material via web search. Imposing "reasonable restrictions" on the Net has certain limitations. This fact needs to be appreciated, and accordingly, a legal framework based on the principle of "reasonableness and due care" has to be adopted. This question was examined by the Supreme Court in series of Writ Petitions, like ***ShreyaSinghalvs Union of India,***[187]***Dilip Kumar Tulsidas Shah vs Union of India,***[188] ***Rajeev Chandrashekharvs Union of India,***[189] ***Common Cause (A Regd. Society) vs Union of India,***[190] ***PUCL vs Union of India,***[191] ***Mouthshut.com (India) Pvt. Ltd vs Union of India,***[192]***TalimaNasrinvs State of Uttar Pradesh,***[193]***ManojOswalvs Union of India,***[194] ***and Internet and Mobile Association of India vs Union of India.***[195]As articulated previously, the question before the court was whether section 66A (Punishment for sending offensive messages through communication service, etc.) of the Information Technology Act was violative of Article 14, 19 and 21 of the Constitution of India? The Court declared section 66A as ultra vires on account of causing chilling effect.

[187]*ShreyaSinghal v Union of India*WP (Crl) No 167 of 2012
[188]*Dilip Kumar Tulsidas Shah v Union of India*WP (C) No 97 of 2013
[189]*Rajeev Chandrashekhar v Union of India*WP (C) No 23 of 2013.
[190]*Common Cause (A Regd Society) v Union of India*WP (C) No 21 of 2013
[191]*PUCL v Union of India*WP (C) No 199 of 2013
[192]*Mouthshut.com (India) Pvt Ltd vUnion of India*WP (C) No 217 of 2013
[193]*TalimaNasrin v State of Uttar Pradesh*WP (Crl) No 222 of 2013
[194]*ManojOswal v Union of India*WP (Crl) No 225 of 2013
[195]*Internet and Mobile Association of India v Union of India*WP (C) No 758 of 2014

The relevant extract of the Supreme Court judgment in ***ShreyaSinghal case*** referring to section 66A being violative of freedom of speech and expression is reproduced for better understanding of the judicial interpretation of Article 19 protecting freedom of speech and expression over Internet.

1.5 FREEDOM OF SPEECH AND EXPRESSION

The Preamble of the Constitution of India inter alia speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be overemphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.

Various judgments of this Court have referred to the importance of freedom of speech and expression both from the point of view of the liberty of the individual and from the point of view of our democratic form of government. For example, in the early case of ***RomeshThapparvs State of Madras,***[196] this court states that freedom of speech lay at the foundation of all democratic organizations. In ***Sakal Papers (P) Ltd. vs Union of India,***[197] a Constitution Bench of this Court said freedom of speech and expression of opinion is of paramount importance under a democratic constitution which envisages changes in the composition of legislatures and governments and must be preserved. In a separate concurring judgment Beg.J.said, in ***Bennett Coleman & Co. vs Union of India,***[198]that the freedom of speech and the press is the Ark of the Covenant of Democracy because public criticism is essential to the working of its institutions.

Equally, in ***S. Khushboovskanniamal,***[199] this court stated, in paragraph 45, that the importance of freedom of speech and expression though not absolute was necessary as we need to tolerate unpopular views. This right required the free flow of opinions and ideas essential to sustain the collective life of the citizenry. While an informed citizenry is a pre-condition for meaningful governance, the culture of open dialogue is generally of great societal importance.

[196] *RomeshThappar v State of Madras*[1950] SCR 594 [602]
[197] *Sakal Papers (P) Ltd v Union of India*[1962] 3 SCR 842 [866]
[198] *Bennett Coleman & Co v Union of India*[1973] 2 SCR 757 [829]
[199] *S Khushboo vkanniamal*[2010] 5 SCC 600

Justice Brandeis, in his famous concurring judgment in ***Whitney vs California,***[200] said:

"Those who won our independence believed that the end of the state was to make men free to develop their faculties and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government. They recognized the risks to which all human institutions are subject. But they knew that order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones. Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law-the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.

Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears. To justify suppression of free speech, there must be reasonable ground to fear that serious evil will result if free speech is practised. There must be reasonable ground to believe that the danger apprehended is imminent. There must be reasonable ground to believe that the evil to be prevented is a serious one.[201] Every denunciation of existing law tends in some measure to increase the probability that there will be a violation of it. Condonation of a breach enhances the probability. Expressions of approval add to the probability.

[200] *Whitney v California*71 L Ed 1095
[201] *Whitney v. California* | US Law | LII / Legal Information <https://www.law.cornell.edu/supremecourt/text/274/357>

Propagation of the criminal state of mind by teaching syndicalism increases it. Advocacy of lawbreaking heightens it still further.[202] But even advocacy of violation, however reprehensible morally, is not a justification for denying free speech where the advocacy falls short of incitement, and there is nothing to indicate that the advocacy would be immediately acted on. The wide difference between advocacy and incitement, between preparation and attempt, between assembling and conspiracy, must be borne in mind. In order to support a finding of the clear and present danger, it must be shown either that immediate serious violence was to be expected or was advocated, or that the past conduct furnished reason to believe that such advocacy was then contemplated."

This leads us to a discussion of what is the content of the expression "freedom of speech and expression". There are three concepts which are fundamental in understanding the reach of this most basic of human rights. The first is discussion, the second is advocacy, and the third is incitement. Mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of Article 19(1)(a).[203] It is only when such discussion or advocacy reaches the level of incitement that Article 19(2) kicks in. It is at this stage that a law may be made curtailing the speech or expression that leads inexorably to or tends to cause public disorder or tends to cause or tends to affect the sovereignty & integrity of India, the security of the State, friendly relation with foreign States, etc. Why it is important to have these three concepts in mind is because most of the arguments of both petitioners and respondents tended to veer around the expression "public order".

1.6 LET'S SUM UP

In this chapter, we have studied the concept of reasonable restrictions with respect to Article 19 of the Indian Constitution along with the Freedom of Expression and the Internet. We also discussed the concept with a plethora of case laws and finally we ended the discussion with Freedom of Speech and Expression.

[202]Brandeis Concurring With Holmes in *Whitney v. California* <https://firstamendmentwatch.org/history-speaks-brandeis-concurring-holmes-whitney-v-california-1927/>
[203]Justice Deepak Gupta's speech on sedition law being abused <https://theprint.in/opinion/heres-the-text-of-justice-deepak-guptas-speech-on-sedition-law-being-abused-and-misused/288439/>

1.7 FURTHER READING

- Seervai, H.M., Constitutional Law of India: A Critical Commentary, Vol. 1 (1975), N.M. Tripathi, Bombay.
- *Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79(1) New York University Law Review, 1 (2009).*
- *Eugene Volokh, Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex , (February12, 2011).*
- *Durga Das Basu, Vol. 2, Commentary on the Constitution of India, 2401 (8th edn., 2007).*

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What does Article 19 of the Indian Constitution state?

The Art. 19 uses the expression *'freedom'* and mentions the several form and aspects of it, which are secured to individuals, together with the limitations that could be, placed upon them in the general interest of the society.

2) Sum up the preamble of the Indian constitution?

The Preamble of the Constitution of India inter alia speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be overemphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.

3) What are the 3 concepts which are fundamental in understanding that reaches to human rights?

The first is discussion, the second is advocacy, and the third is incitement.

4) What is the outcome of ShreyaSinghal case?

The Court declared section 66A as ultra vires on account of causing chilling effect.

1.9 ACTIVITY

Explain the concept of reasonable restrictions along with Freedom of speech and expression with relevant case laws? (1000 words)

Unit 2: Examination of Rights Under Indian Laws

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Analyzing right under the Indian laws

1.4 Analyzing different concepts given in ShreyaSinghal Case

1.5 Indian Cyber law and social media

1.6 The Road Ahead

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Status of Freedom of Speech and Expression under Indian Constitution
- Grounds on which laws can be made to impose reasonable restrictions in the exercise of the right of free speech and expression
- Provisions of the Information Technology Act, 2000, which are being used to tackle the problems arising

1.2 INTRODUCTION

Certain rights are given to individuals by mere reason of being born, and freedom of speech and expression is one such right. Freedom of expression is one of the basic principles of liberty,

society as well as a healthy democracy. Various international charters, declarations, conventions like Universal Declaration of Human Rights, International Convention on Civil and Political Rights, European Convention on Human Rights and Fundamental Freedoms, also advocate in support of this right and protect the same.[204] In the Indian legal matrix, this right of freedom of speech and expression finds place as one of the Fundamental Rights under the Indian Constitution, which collectively are known to be one of the parts of the basic structure of our Constitution.

1.3 ANALYZING RIGHT UNDER THE INDIAN LAWS

Under Indian legal regime, the right finds a place under Article 19 (1) (a) and is read with Article 19 (2), where the latter contains the grounds on which the reasonable restrictions on the exercise of the right can be imposed. Article 19 (1) (a) states that "all citizens shall have the right to freedom of speech and expression".

As it is a well-recognized principle of our Constitution that certain fundamental rights are available to only citizens of the country, whereas others are available to all the people irrespective of whether they are the citizens of this country or not. Article 19, as evident from the plain reading itself, is applicable and available to citizens only, and thus non-citizens aren't entitled to the rights encapsulated under Article 19.

However, this right is not absolute in nature and the grounds on which the laws can be made so as to impose reasonable restriction in the exercise of the right of freedom of speech and expression (as given under Article 19 (1) (a)) are given under Article 19 (2).[205] These are:

- Sovereignty and Integrity of India ;
- Security of the State ;
- Friendly relations with foreign States ;
- Public Order ;
- Decency ;

[204] M Yar, Cybercrime and Society SAGE, 2016
[205] RBroadhurst, "Developments in the globallLaw enforcement of cybercrime," Policing: An International Journal of Police Strategies and Management, vol29, no 3, pp 408–433, 200 6 <https://doi.org/10.1108/13639510610684674>

- Morality ; or
- In relation to contempt of court, defamation, incitement to an offence.

Under the IT Act also, the power to block certain websites and computer resources (and thus in a way, curtailment on the right of freedom of speech and expression), has been given to the Central Government. Section 69A of the IT Act empowers the Central Government or any officer specially authorized by it to order any government agency or intermediary to block access, by public, to certain information which is generated by, stored in or transmitted by computer resources) in the interest of the defence of India, its sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order or for preventing incitement to the commission of an offence. Further, the details of the procedural safeguards that need to be followed while blocking access have been mentioned in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (hereinafter referred to as the Blocking Rules).

1.4 ANALYZING DIFFERENT CONCEPTS GIVEN IN SHREYA SINGHAL CASE

One of the points which came up for the consideration of the court was whether the restrictions mentioned under Article 19(2) also apply to speech and expression made with the use of internet, or in the context of freedom of press/media, whether the restrictions apply to electronic media as well. This point came up in the Supreme Court during arguments in the case of *ShreyaSinghal v. Union of India (Writ Petition (Criminal) 167 of 2012)*, and the argument that Article 19(2) doesn't apply to electronic media was rejected by the Hon'ble Supreme Court after placing reliance on its judgment in the case of *Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal*, wherein the Apex Court held that "The 'right to communicate' includes right to communicate through any media that is available whether print or electronic or audiovisual such as advertisement, movie, article, speech etc.". Placing heavy reliance on this previously decided case of the Apex Court, Justice Nariman in the ShreyaSinghal case pronounced that "The virtues of the electronic media cannot become its enemies."[206]

[206] R P Kataria& S K PSrinivasan,Cyber Crimes Law, Practice & Procedure along with Cyber Evidence and Information Technology Act, 2000 with Allied Rules (New ed 2014)

However, when it comes to cyberspace, the Hon'ble Supreme Court did differentiate it with any other medium and upheld that the Internet is a distinct medium. The factors relied on by the court for the same were "global reach of Internet", "impossibility of pre-censorship" (because anyone can publish their content), "possibility of the use of new technologically advanced methods to modulate the content", "lack of code of ethical conduct" and "individualised production" (of the content). And hence the Court affirmed that electronic medium "may warrant a greater regulation over licensing and control and vigilance on the content of the program telecast".

After analyzing and settling on the points above mentioned along with a few others, on the question of validity of Section 66A of the IT Act, 2000, the Supreme Court upheld that the said provision can't be justified as placing reasonable restrictions on the exercise of right on the grounds mentioned under Article 19 (2). The Court then went on to analyse how the provision couldn't be said to be justified under each grounds of Article 19(2). To the best far outreach, out of all the grounds mentioned under Article 19(2), it can be confused to be justified undergrounds of public order, defamation, incitement to an offence, decency and morality and nothing else. The Court refused to accept that the impugned provision would be justified under the interests of 'public order' because the scope of the provision was so large that it covered within its ambit, both messages to individuals as well as mass messages. Then, it refused the impugned provision, the protection under the exception for defamation because the provision didn't concern itself with injury to reputation. For refusing the provision to be considered as a valid exception on the ground of prevention of 'incitement to an offence', the Court gave the reason that it seeks to control all information irrespective of whether it 'incites' anyone or not. Lastly, on the exception on the ground of decency or morality, the court didn't give the provision the defence of the mentioned grounds because the provision made an only oblique reference to those concepts.[207]

While striking down the provision, the Court also pointed out that the language of the provision and also the terminology referred to in Section 66A is vague, undefined and open-ended. For instance, terms like 'annoying', 'inconvenience' and 'grossly offensive' which have been used in the provision do not point to any specific offence and hence creates confusion for both law

[207]Obar, J A and Wildman, S (2015) Social media definition and the governance challenge: An introduction to the special issue. TELECOMMUNICATIONS POLICY, 39(9), 745-750

enforcement agencies and the general public about what is permitted under the then impugned provision and what is not.

In a country like India, which has recently switched on and has started using the internet at a rapid increase, and a lot of people starting to express their views over the internet through blogs, vlogs, social networks, it is a very important decision and is much appreciated. Also, in a societal set up like ours where the precedent has been set in a very negative way which advocates for suppressing the dissent which is against the people at power, this judgment has given the people a lot of moral support and assurance and will encourage people to express their views over the internet without any fear of vengeance.

1.5 INDIAN CYBER LAW AND SOCIAL MEDIA

At present, there is no specific legislation in our country which deals directly with social media. However, several provisions of a bundle of laws which collectively are called cyber laws could be sought for redressal in case of violation of any rights in the cyberspace, internet and social media.[208] Most important of them under the Information Technology Act, 2000 are listed below:-

1. Sections 65, 66, 66A, 66C, 66D, 66E, 66F, 67, 67A and 67B of Chapter XI of the IT Act, 2000, contain punishments for computer-related offences, and they can also be committed through social media, the concerned offences are: tampering with computer source code, committing computer-related offences given under Section 43, sending offensive messages through communication services, identity theft, cheating by personation using computer resource, violation of privacy, cyber terrorism, publishing or transmitting obscene material in electronic form, material containing sexually explicit act in electronic form, material depicting children in sexually explicit act in electronic form, respectively.[209]
2. Under Section 69 of the IT Act, 2000, the Central or a State Government has been given the power to issue directions for interception or monitoring or decryption of any

[208]Soomro, Tariq &Hussain, Mumtaz.(2019). Social Media-Related Cybercrimes and Techniques for Their Prevention.Applied Computer Systems. 24. 9-17. 10.2478/acss-2019-0002
[209]Social Media And Freedom of Speech And Expression
<http://www.legalserviceindia.com/legal/article-426-social-media-and-freedom-of-speech-and-expression.html>

information through any computer resource in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, for preventing incitement to commission of any cognizable offence, for investigation of any offence.[210]

3. Section 69A of the IT Act, 2000, grants power to the Central Government to issue directions to block public access of any information through any computer resource on similar grounds.
4. Under Section 69B of the IT Act, 2000, the Central Government has been empowered to issue directions to authorize any agency to monitor and collect traffic data or information through any computer resource for cybersecurity.
5. Section 79 of the IT Act, 2000, deals with the liability of intermediary. An intermediary shall not be liable for any third party information, data or communication link made available or hosted by him if certain conditions mentioned therein are fulfilled.
6. Section 66A of the Information Technology Act, 2000.

   Section 66A was originally inserted with an intention to tackle the twin problems of spam and cyberstalking. However, the provision became widely infamous due to it being used to crack down on online dissent and political criticism. After the judgment in the case of ShreyaSinghal vs. Union of India (AIR 2015 SC 1523), this provision has been declared unconstitutional but for a better understanding and appreciation of the points regarding judgment as discussed above it is important to have a look at the provision itself.

66A. Punishment for sending offensive messages through communication service, etc.-

Any person who sends, by means of a computer resource or a communication device-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

[210] Nikita Barman, Legal Implications of Cyber Crimes on Social Networking Websites, International Journal of Scientific and Research Publications, Volume 5, Issue 12, December 2015, ISSN 2250-3153 (E-Copy) <http://www.ijsrp.org/research-paper-1215/ijsrp-p4850.pdf>

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with a fine.

Explanation.–For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.[211]

1.6 THE ROAD AHEAD

Due to absence of any specific law to deal the matter in hand, there is a very wide scope of misuse of the laws, and misuse of laws is not something which is alien to our system. Even after Section 66A was struck down and declared unconstitutional by the Hon'ble Supreme Court, there have been instances wherein people sharing jokes, memes, posts, or their views have been booked unjustly.[212] Though there may be a disagreement amongst people as to the reason behind these cases being registered, with some blaming it on the unawareness of the police officials regarding the striking down of Section 66A, while some of them alleging the unfair intentions of the officials and thus making a sham case of sedition or defamation etc., whereas some terming it as a means of political vendetta, but all would agree that whatever might be reason for this misuse, it can definitely be curbed by the coming in force of a proper legislation dealing with the matter specifically.

[211]Seema D Trived, Ms. ChandaniKathad, Analytical Study Of Cyber Threats In Social Networking, Proceedings of International Conference on Computer Science Networks and Information Technology Held on 23rd-24th January 2016, in Pattaya, ISBN: 9788193137338 (http://www.innovativeresearchpublication.com/documents/papers/jan_pattaya%202016/pdf%206.pdf)

[212]DrJyoti Rattan, Bharat's Cyber Laws & Information Technology, Bharat, Fifth Edition, 2015, ISBN: 978-93-5139-240-8

1.7 LET'S SUM UP

In this chapter, we have studied how freedom of speech and expression is analyzed under the Indian Laws along with the different concepts given in ShreyaSinghal Case. We also discussed about the Indian Cyber law and social media concepts and finally, ended the discussion with the road map after striking down Section 66A of the I.T. Act.

1.8 FURTHER READING

- Feldman, David, Civil Liberties and Human Rights in England and Wales, 2nd Edition, Oxford University Press, UK, 2002, at 763.
- Baker C E, Human Liberty and Freedom of Speech, Oxford University Press, London, 1989 at p 73.
- Bernardino, Raul. (2015). The Freedom of Speech in Cyberspace. 10.13140/RG.2.1.1496.0089.
- A. J. Feldman, A. Blankstein, M. J. Freedman, and E. W. Felten, ―Social networking with frientegrity: Privacy and integrity with an untrusted provider‖, in USENIX Security Symposium, pp. 647–662, 2012.
- E. Novak and Q. Li, ―A survey of security and privacy in online social networks, College of William and Mary Computer Science Technical Report , 2012.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Whether a citizen of Malaysia who has been residing in India for last 10 years, move to Supreme Court for the enforcement of right under Article 19 (1) (a) by way of writ petition?**

Since, in the hypothetical situation given above, the person concerned is a citizen of Malaysia and not of India, and certain Fundamental Rights, one of which is Article 19, is available to citizens only, the person concerned is not entitled to this as a Fundamental Right. And since the High Court or the Supreme Court is approached by way of writ petition for the enforcement of any Fundamental Right, this person cannot move to Supreme Court for enforcement of right under 19(1)(a) by way of the writ petition.

2. **What are the grounds which are mentioned under the Indian Constitution on which a reasonable restriction on the exercise of the right of free speech and expression be placed?**

   The grounds under which reasonable restrictions can be placed in the exercise of the fundamental freedom of speech and expression are covered under Article 19 (2). These grounds are Sovereignty and Integrity of India; Security of the State; Friendly relations with foreign States; Public Order; Decency; Morality; or In relation to contempt of court, defamation, incitement to an offence.

3. **Does International Covenant on Economic, Social and Cultural Rights mention about the right of speech and expression to be ensured by the member/signatory nations?**

   No, the International Covenant on Economic, Social and Cultural Rights doesn't. But, the Universal Declaration of Human Rights and the International Convention on Civil and Political Rights does, under Article 19 of both of them.

4. **Whether intermediary has a joint and several liability for information posted upon its portal?**

   No, as mentioned under Section 79 of the IT Act, the intermediary is absolved of all of its liability if it has complied with certain conditions prescribed and referred to in the provision. The Central Government has made separate rules, known as Information Technology (Intermediaries guidelines) Rules, 2011, which requires to be complied with for it being absolved of the liabilities.

5. **Whether the intention of the legislature to bring Section 66A of the IT Act was to suppress dissent against the government?**

No, intention of the legislature was a noble one. Instead, it was to tackle the twin problems of spam and cyberstalking. However, as per the data available, the provision has majorly been used for satisfying the political vendetta and for suppressing the political dissent.

1.10 ACTIVITY

Write about the incidents where cases against individuals have been filed for writing or sharing posts or messages relating to political issue or angle, provided they must have happened after the Supreme Court declared Section 66A as unconstitutional, and the recent individual updates about all of them. In the light of the same, analyse the provisions which have been misused due to any reason whatsoever. (1000 words)

Unit 3: The Legislative Responses in Cyberspace

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Cyberspace: To legislate or not

1.4 The Legislative Response I

1.5 The Verdict

1.6 The Legislative Response II

1.7 The Verdict

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The Legislative responses of cyberspace
- The enactment of Community Decency Act
- The verdicts of different cases and opinions of courts

1.2 INTRODUCTION

With the advent of the Internet, there has been a subtle shift in the law-making as well, i.e., the law is now no longer meant for the man only, it is now for the machines as well. For example, the law has been able to recognize the computer as a tool in criminal activity.

A computer could now be referred to as a 'weapon of offence' as well as a 'victim of crime'. What is being witnessed is – the emergence of cyberspace jurisprudence.

1.3 CYBERSPACE: TO LEGISLATE OR NOT

Internet is an open system of communication with unlimited choices. It has its own culture, which is non-hierarchical, open and dynamic. It is, in fact, anti-thesis of whatever the global society has experienced so far. So, what would be the 'philosophy of cyberspace law'? The primary objective of such a philosophy should be to understand the dynamics of this emerging culture. Also, the lawmakers need to address the issues with an open mind without any preconceived notions, biases and restrictions.

The question that the emerging cyberspace has thrown in is that – does cyberspace need a law? If yes, what should be its parameters? Should the 'new' legislation be just an extension of the 'old' legislation or should it reflect an understanding of the emerging medium? And lastly, what should be the response of the courts in safeguarding citizens' constitutional guarantees via-à-vis the new medium?

1.4 THE LEGISLATIVE RESPONSE I

One of the earliest legislative responses to the development of the Internet was the introduction of the Communications Decency Act, 1996 (CDA) by the US government.

Section 502 of the CDA amended sections 223(a) and (d) of Title 47 of the United States Code (USC). These provisions prohibited the making of obscene or 'indecent' material and its transmission to a minor by means of a telecommunication device, and the use of an interactive computer service to send or display 'patently offensive' material to minors.

Section 223(a), the indecency provision, subjects to criminal penalties of imprisonment of no more than two years, or a fine or both, anyone who:[213]

[213] *American Civil Liberties Union v Reno*, 929 F Supp 824 <https://law.justia.com/cases/federal/district-courts/FSupp/929/824/1812782/>

(1) In interstate or foreign communications, by means of a telecommunications device knowingly

(i) Makes, creates, or solicits, and

(ii) Initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

(2) Knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity.[214]

Section 223(d), the 'patently offensive' provision, subjects to criminal penalties anyone who:

(1) In interstate or foreign communications knowingly

(A) Uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) Uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such a service placed the call or initiated the communication.

(2) Knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity.

The aforesaid provisions were considered as an unacceptable intrusion into the right to free speech, which is protected by the First Amendment to the US Constitution, which states that the "Congress shall make no law abridging the freedom of speech". Subsequently, the American Civil Liberties Union (ACLU) filed a case challenging the legal validity of the aforesaid

[214] *Reno v. ACLU* | US Law | LII / Legal Information Institute <https://www.law.cornell.edu/supremecourt/text/521/844>

provisions. The case came to known as ***American Civil Liberties Union vs Janet Reno, Attorney-General of the United States***[215] ***(ACLU vs Reno 1).***

1.5 THE VERDICT

THE DISTRICT COURT

The District Court for the Eastern District of Pennsylvania fount that whilst the First Amendment to the Constitution enshrined the principle of freedom of speech, this did not apply to child pornography and 'obscenity' which have 'no constitutional protection'.[216]

The court observed, because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between speakers and listeners on the Internet. Chat rooms, email and newsgroups are an interactive form of communication, providing the user with the opportunity both to speak and to listen/

It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there. The Internet is, therefore, a unique and wholly new medium of worldwide human communication.

Communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident'. A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases, the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content.

District Judge Dalzell opined, "The internet is a new medium of mass communication. As such, the Supreme Court's First Amendment jurisprudence compels us to consider the special qualities

[215] *American Civil Liberties Union v Janet Reno, Attorney-General of the United States* 929 F Supp 824 (EDPa)[1996]
[216] *Alliance for Community Media v FCC* 56 F 3d 105 (112) (DC Cir)[1995]

of this medium in determining whether the CDA is a constitutional exercise of governmental power. I conclude that the CDA is unconstitutional and that the First Amendment denies Congress the power to regulate protected speech on the Internet.

The CDA will, without doubt, undermine the substantive, speech-enhancing benefits that have flowed from the Internet. The diversity of the content will necessarily diminish as a result.

Some of the dialogue on the Internet surely tests the limits of conventional discourse. Speech on the Internet can be unfiltered, unpolished and unconventional, even emotionally charged, sexually explicit and vulgar – in a word 'indecent' in many communities. But we should expect such speech to occur in a medium in which citizens from all walks of life have a voice. We should also protect the autonomy that such a medium confers to ordinary people as well as media magnates.

The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion.

The absence of governmental regulation of Internet content has unquestionably produced a kind of chaos, but as one of the plaintiffs' experts put it with such resonance at the hearing: what achieved success was the very chaos that Internet is. The strength of the Internet is that chaos".

Just as the strength of the Internet is chaos, so strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment Protects".[217]

THE SUPREME COURT

The US government appealed the district court's decision to the Supreme Court, which affirmed, accepting the court's conclusion that 'the CDA places an unacceptably heavy burden on protected speech, and the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision'. ***Reno vs ACLU,[218] (Reno II).***It held that, although the government has an interest in protecting children from potentially harmful

[217]Remember the "borderless" Internet? It's officially dead <https://arstechnica.com/tech-policy/2011/11/the-borderless-internet-is-officially-dead/>
[218]*Reno vs ACLU*521 US 844 [1997]

materials, the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send or receive.

Justice Stevens opined that:

"The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns."[219]

"The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in ***Ginsberg and Pacifica,*** the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messaged or displaying them on their own computers in the presence of minors.[220] The general, undefined terms "indecent" and "patently offensive" cover large amounts of non-pornographic material with serious educational or other value".

1.6 THE LEGISLATIVE RESPONSE II

Later in 1998, the US Congress came out with another enactment, the Child Online Protection Act (COPA). It was a second attempt by the Congress to regulate the dissemination to minors of indecent material on the Web/Internet. The "COPA" was signed into law on October 21, 1998.

[219]Washingtonpost.com: Statute 'Silences Some Speakers'
<https://www.washingtonpost.com/wp-srv/national/longterm/supcourt/stories/062797_d.htm>
[220]*Reno v American Civil Liberties Union* : 521 U.S. 844
<https://supreme.justia.com/cases/federal/us/521/844/>

COPA applies broadly on its face to any website that, in the regular course of business, communicates any speech that includes any material that is harmful to minors. COPA defines a person "engaged in the business" as one who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labour to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income).[221]

Under (47 U.S.C. section 231(e)(6)), COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that[222] –

(A) The average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) Depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) Taken as a whole, lacks serious, literary, artistic, political, or scientific value for minors.

Under COPA, a minor is defined as one under age seventeen. (47 U.S.C. section 231(e)(7)).

COPA also provides Web publishers subject to the statute with affirmative defenses. If a Web publisher "has restricted access by minors to material that is harmful to minors" through the use of a "credit card, debit account, adult access code, or adult personal identification number, a digital certificate that verifies age or by any other reasonable measures that are feasible under available technology," then no; liability will attach to the Web publisher even if a minor should nevertheless gain access to restricted material under COPA. (47 U.S.C. section 231(c)(1)).

[221]Third Circuit Court of Appeals Decision in *ACLU v Reno II*
<https://www.aclu.org/legal-document/third-circuit-court-appeals-decision-aclu-v-reno-ii>
[222]*ASHCROFT vAMERICAN CIVIL LIBERTIES UNION*
<https://www.law.cornell.edu/supct/html/00-1293.ZO.html>

COPA violators face both criminal (maximum fines of $50,000 and a maximum prison term of six months, or both) and civil (fines of up to $50,000 for each day of violation) penalties. (47 U.S.C. section 231(a)(2)).

1.7 THE VERDICT

THE DISTRICT COURT

On the very next day of signing of COPA, i.e., on October 22, 1998, plaintiffs (ACLU et al) filed this suit in the United States District Court for the Eastern District of Pennsylvania, alleging, inter alia, that COPA violated the First Amendment to the Constitution. Plaintiffs sought an injunction to prevent its enforcement. The case came to known as ***American Civil Liberties Union vs Janet Reno, Attorney-General of the United States,[223] ACLU vs Reno (Reno III).***

On February 1, 1999, following an evidentiary hearing, the district court preliminarily enjoined enforcement of COPA, which imposes severe criminal and civil sanctions on persons who by means of the World Wide Web, make any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." (47 U.S.C. section 231(a)(1)-(3)).

The majority of factual findings and conclusions by the district court mirror those found in ***American Civil Liberties Union v Reno (Reno I).*** It held that it would be prohibitively expensive for some commercial speakers who have websites to verify that their users are adults. These limitations must inevitably curtail a significant amount of adult communication on the Internet. Further, it held that respondents were likely to succeed on their claim as COPA violated the First Amendment. "COPA imposes a burden on speech that is protected for adults," and because the government could not prove that COPA is the least restrictive means available to achieve the goal of restricting the access of minors too (harmful to minors) material.

THE COURT OF APPEALS

[223] *American Civil Liberties Union v Janet Reno, Attorney-General of the United States* 31 F Supp 2d 473 (E D Pa)[1999]

Against the district court's order, in ***Reno III,*** the appellant (Reno) moved to the US Court of Appeals for the Third Circuit ***(American Civil Liberties Union vs Reno, (Reno IV)).***[224]On June 22, 2000, the court upheld the granting of injunction on the basis of likely unconstitutionality.

The court of appeals did not reject the district court's rationale, but rather held that "because the standard by which COPA gauges whether material is 'harmful to minors' is based on identifying 'contemporary community standards' the inability of Web publishers to restrict access to their websites based on the geographic locale of the site visitor, in and of itself, imposes an impermissible burden on constitutionally protected First Amendment speech."

The Court of Appeals concluded that COPA's use of "contemporary community standards" to identify material that is harmful to minors rendered the statute substantially overbroad. Because "Web publishers are without any means to limit access to their sites based on the geographic location of particular Internet users," the Court of Appeals reasoned that COPA would require "any material that might be deemed harmful by the most puritan of communities in any state" to be placed behind an age or credit card verification system. Hypothesizing that this step would require Web publishers to shield "vast amounts of material," the Court of Appeals was "persuaded that this aspect of COPA, without reference to its other provisions, must lead inexorably to a holding of a likelihood of unconstitutionality of the entire COPA statute."[225]

THE SUPREME COURT

The US Supreme Court granted the Attorney General's petition for ***certiorari,*** to review the Court of Appeals' determination that COPA likely violates the First Amendment because it relies, in part, on community standards to identify material that is harmful to minors, and now vacate the Court of Appeals' judgment.

CASE	**COURT**	**LEGISLATION IN QUESTION**	**VERDICT**
American Civil Liberties Union,	The District Court for the Eastern District of	Communications Decency Act, 1996	The CDA is unconstitutional and

[224]*American Civil Liberties Union v Reno*217 F 3d 162 (CA) 3 [2000]
[225]Indecency Online | Freedom Forum Institute <https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/indecency-online/>

(ACLU) vs Janet Reno, Attorney-General of the United States (Reno I)	Pennsylvania.	(CDA)	that the First Amendment denies Congress the power to regulate protected speech on the Internet.
Reno vs ACLU, (Reno II)	US Supreme Court	Communications Decency Act, 1996	The CDA suppresses a large amount of speech that adults have a constitutional right to send or receive. It is patently invalid and unconstitutional.
ACLU vs Reno (Reno III)	District Court for the Eastern District of Pennsylvania	The Child Online Protection Act, 1998 (COPA)	The COPA imposes a burden on speech that is protected for adults. The court preliminarily enjoined enforcement of COPA.[226]
ACLU vs Reno (Reno IV)	US Court of Appeals for the Third Circuit.	The Child Online Protection Act, 1998 (COPA)	COPA's use of contemporary community standards to identify material that is harmful to minors rendered the statute substantially overbroad.

[226]First Amendment wins another round online | Salon.com <https://www.salon.com/1999/02/02/feature_232/>

1.8 LET'S SUM UP

In this chapter, we have studied the legislative responses of cyberspace along with the enactment of community decency act, 1996. We discussed the act with case laws along with verdicts and opinions of different courts. Finally, we ended the discussion with a brief of all the cases discussed along with the findings of the court.

1.9 FURTHER READING

- U.S. Department of Commerce, National Telecommunications and Information Administration, A Nation Online: How Americans Are Expanding Their Use of the Internet at 1, 13 (Feb. 2002)
- National Center for Education Statistics, Internet Access in U.S. Public Schools and Classrooms: 1994-2001 at 3 (September 2002).
- Corporation for Public Broadcasting, Connected to the Future (March 2003).
- See In the Matter of Federal-State Joint Board on Universal Service, Children's Internet Protection Act, CC Docket No. 96-45, Order, FCC 03-188 (rel. July 24, 2003) (implementation timing modifications).
- Davidson, Julia & Justice, Patrick & Prevention, South & Institute, Society & Kingdom, United & Davison, Patrick & America, United & Asia, Emma & Kingdom, Majida&Razai, Sara &Scally, Mia & (Australia, Dr. (2016). Child Online Protection in the MENA Region. 10.13140/RG.2.2.36165.65761.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the earliest development of the Internet?

One of the earliest legislative responses to the development of the Internet was the introduction of the Communications Decency Act, 1996 (CDA) by the US government.

2) **How is the word indecency has been defined under the Communications Decency Act?**

Section 223(a), the indecency provision, subjects to criminal penalties of imprisonment of no more than two years, or a fine or both.

3) **What was the enactment that was brought to light by the US Congress?**

In 1998, the US Congress came out with another enactment, the Child Online Protection Act (COPA).

4) **How does COPA define material that is harmful to minors under the act?**

COPA defines "material that is harmful to minors" as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene.

1.11 ACTIVITY

Elucidate the legislative responses of cyberspace with different case laws and the amendments made? (1000 words)

Unit 4: National Sovereignty and Freedom of Expression

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Yahoo! Inc.: The Fact File

1.4 The Complaint

1.5 The Verdict I

1.6 Yahoo's! Response

1.7 The Question before the experts

1.8 The Expert opinion

1.9 The Verdict II

1.10 The Verdict III

1.11 What Next?

1.12 The Message

1.13 Let's sum up

1.14 Further reading

1.15 Check your progress: Possible answers

1.16 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The fact file of Yahoo! Inc.
- The question before the experts
- The expert opinion and the message from Yahoo!'s case

1.2 INTRODUCTION

It would be really interesting to look into the interplay of law and polity in determining the jurisdictional issues flowing from nationalistic constitutional guarantees'. So far, there have only been few cases highlighting the conflict between nationalistic constitutional guarantees' in the Internet space, i.e., conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of two different nation-states. The case involving Yahoo! Inc. and organizations dedicated to eliminating anti-Semitism has all such ingredients.

1.3 YAHOO! INC.: THE FACT FILE

Yahoo! is an Internet service provider that operates various Internet websites and services that any computer user can access at *http://www.yahoo.com*.[227]It is an all-purpose portal providing services such as Internet search engine, email, an automated auction site, personal web page hostings, shopping services, chat rooms, and a listing of clubs that individuals can create or join.

Yahoo! services ending in the suffix, ".com," without an associated country code as a prefix or extension use the English language and target users who are residents of, utilize servers based in and operate under the laws of the United States.[228] Yahoo! subsidiary corporations operate Yahoo! sites and services in other nations, including, for example, Yahoo! France, yahoo!India,and Yahoo! Spain. Each of these regional web sites contains the host nations' unique two-letter code as either a prefix or a suffix in its URL (e.g., Yahoo! France is found at *http://www.yahoo.fr*and Yahoo! India at *http://www.yahoo.co.in*). Yahoo!'s regional sites use the local region's primary language, target the local citizenry, and operate under local laws. Any

[227]*Yahoo!, Inc v LICRA* - Tom W Bell
<http://www.tomwbell.com/NetLaw/Ch03/YahoovLICRA.html>
[228]Legal Risk Management in Electronic Commerce - Chapter 5
<http://www.legalriskmanagement.net/book/5.html>

computer user with Internet access is able to post materials on many of these Yahoo! sites, which in turn are instantly accessible by anyone who logs on to Yahoo!'s Internet sites.[229]

Yahoo!'s auction site allows anyone to post an item for sale and solicit bids from any computer user from around the globe. Yahoo! records when a posting is made and after the requisite time period lapses sends an e-mail notification to the highest bidder and seller with their respective contact information. Yahoo! is never a part to a transaction, and the buyer and seller are responsible for arranging privately for payment and shipment of goods. Yahoo! monitors the transaction through limited regulation by prohibiting particular items from being sold (such as stolen goods, body parts, prescription and illegal drugs, weapons, and goods violating U.S. copyright laws or the Iranian and Cuban embargos) and by providing a rating system through which buyers and sellers have their transactional behavior evaluated for the benefit of future consumers. Yahoo! informs auction sellers that they must comply with Yahoo!'s policies and may not offer items to buyers in jurisdictions in which the sale of such item violates the jurisdiction's applicable laws.

Yahoo! does not actively regulate the content of each posting, and individuals are able to post and have in fact posted, highly offensive matter, including Nazi-related propaganda and Third Reich memorabilia, on Yahoo!'s auction sites.

1.4 THE COMPLAINT

On or about April 5, 2000, La LigueContre Le Racisme Et l'Antisemitisme (The League Against Racism and Antisemitism – "LICRA") sent a "cease and desist" letter to Yahoo!'s Santa Clara headquarters informing Yahoo! that the sale of Nazi and Third Reich related goods through its auction services violate French law. LICRA threatened to take legal action unless Yahoo! took steps to prevent such sales within eight days. Defendants subsequently filed a civil complaint against Yahoo! in the Tribunal de Grande Instance de Paris (the "French Court").[230]

[229]Ibid.
[230]Aditya, S &Yadav, Dr Raj (2015) CYBER LAW: AN ANALYSIS. Plebs Journal of Law 1 69-80

1.5 THE VERDICT I

The French Court found that approximately 1,000 Nazi and Third Reich related objects, including Adolf Hitler's *Mein Kampf, The Protocol of the Elders of Zion* (an infamous anti-Semitic report produced by the Czarist secret police in the early 1900's), and purported "evidence" that the gas chambers of the Holocaust did not exist were being offered for sale on Yahoo.com's auction site. Because any French citizen is able to access these materials on Yahoo.com directly or through a link on Yahoo.fr, the French Court concluded that the Yahoo.com auction site violates Section R645-1 of the French Criminal Code, which prohibits the exhibition of Nazi propaganda and artifacts for sale.

An order was made on May 22, 2000 against the companies Yahoo! France and Yahoo! Inc. by the County Court of Paris in the following terms:[231]

"We order the company Yahoo! Inc. to take all measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi objects and to any other site or service that may be construed as constituting an apology for Nazism or contesting the reality of Nazi crimes;

We order the company Yahoo! France to warn any surfer visiting Yahoo.fr, even before use is made of the link enabling him or her to proceed with searches on Yahoo.com, that if the result of any search, initiated either through a tree structure or by means of keywords, causes the surfer to point to sites, pages or forum of which the title and/or content constitutes a violation of French law, as applies to the viewing of sites making an apology for Nazism and/or exhibiting uniforms, insignia or emblems resembling those worn or displayed by the Nazis, or offering for sale objects or works whose sale is strictly prohibited in France, the surfer must desist from viewing the site concerned subject to imposition of penalties provided in French legislation or the bringing of legal action against him".

The French Court set a return date in July 2000 for Yahoo! to demonstrate its compliance with the order.

[231] I N T E R I M C O U R T O R D E R made on 20 November 2000
< http://www.kentlaw.edu/perritt/conflicts/frenchorder.pdf>

1.6 YAHOO'S! RESPONSE

Yahoo! asked the French Court to reconsider the terms of the order, claiming that although it easily could post the required warning on Yahoo.fr, compliance with the order's requirements with respect to Yahoo.com was technologically impossible.

The Yahoo! Inc. pointed out that there was no technical solution, which would enable it to comply fully with the terms of the court order. A panel of experts was then designated to enlighten the Court on the various technical solutions that could be implemented by Yahoo! Inc. in order to comply with its order of May 22, 2000.

1.7 THE QUESTION BEFORE THE EXPERTS

The expert opinion was sought, whether it is possible to:

a) Know the geographical origin and nationality of surfers wishing to access its auctions site.
b) Prevent French surfers or surfers connecting from French territory from perusing the description of Nazi objects posted for auction, and even more importantly to prevent them from bidding.[232]

1.8 THE EXPERT OPINION

The experts filed their opinion on November 6, 2000. They opined that:

a) Some 70% of the IP addresses of French users or users residing in French territory are capable of being correctly identified by specialized providers such as InfoSplit, GeoNet or others, using specialized databases. Around 30% of the IP addresses assigned to French users cannot be identified.

[232] Singh, Harman (2018)Cyber squatting and the Role of Indian Courts: A Review 2 18-23

b) Yahoo! displays advertising banners targeted at surfers considered by that company to be French, and that it, therefore, has the technical means to identify them.

c) In addition to the geographical identification already practiced by Yahoo to target its advertising, it would also be desirable to ask surfers whose IP address is ambiguous to make a declaration of nationality. This declaration, given on honour, would only be required of surfers whose IP address cannot be identified as belonging to a French ISP (e.g. multinational ISPs like AOL, address transmitted from an anonymizersite, or encapsulation of an address assigned by an intranet server).

d) At the discretion of Yahoo, this declaration of nationality could be made on the home page of the auctions site, or only in the context of a search for Nazi objects if the word "Nazi" is included in the user's request, immediately before the search engine processes the request. In these circumstances, the consultants consider that it cannot be reasonably claimed that this would have a negative impact on the performance and response time of the server hosting the Yahoo! auctions service.

e) The combination of two procedures, namely geographical identification of the IP address and declaration of nationality, would be likely to achieve a filtering success rate approaching 90%.

1.9 THE VERDICT II

On November 20, 2000, Jean-Jacques GOMEZ, First Deputy Justice Presiding in the County 00/05308 Court of Paris, reaffirmed its order of May 22, 2000, involving *The League against Racism and antisemitism –LICRA and The French Union of Jewish Students (Plaintiffs) vs Yahoo! Inc. and Yahoo France,*[233]*(Respondents)* and held that Yahoo! to comply with the May 22 order within three months or face a penalty of 100,000 Francs (approximately U.S. $13,300) for each day of non-compliance.[234]

The Court overruled the objection of the respondents that it was not competent to make a ruling in this dispute. It observed that "the simple act of displaying such objects (of Nazi ideology) in France constitutes a violation of Article R645-1 of the Penal Code and therefore a threat to

[233]See <www.cdt.org> for the English translation of the court's order
[234]C JURISDICTION TO ADJUDICATE
<http://www.wneclaw.com/internet/foreignjudgments.pdf>

internal public order; Whereas Yahoo! is aware that it is addressing French parties because upon making a connection to its auctions site from a terminal located in France it responds by transmitting advertising banners written in the French language; Whereas a sufficient basis is thus established in this case for a connecting link with France, which render our jurisdiction perfectly competent to rule in this matter; Whereas any possible difficulties in executing our decision in the territory of the United States, as argued by Yahoo Inc., cannot by themselves justify a plea of Incompetence; Whereas this plea (of not competent) will, therefore, be rejected".

1.10 THE VERDICT III

Yahoo! Inc. or Yahoo France did not go for appeal in France against the aforesaid judgment. Later, Yahoo! Inc. (as Plaintiff) approached the District Court of Northern California for summary judgment with the plea that the French court's order was without effect in the United States since its enforcement would violate Yahoo's First Amendment right of free speech.

It argued that it cannot comply with the French order without banning Nazi-related material from Yahoo.com altogether. Yahoo! Inc. contends that such as ban would infringe impermissibly upon its rights under the First Amendment to the United States Constitution. It sought a declaratory judgment that the French Court's orders are neither cognizable nor enforceable under the laws of the United States. Defendants (LICRA, et al) immediately moved to dismiss on the basis that this Court lacks personal jurisdiction over them. That motion was denied.[235]

Jeremy, Fogel, District Judge observed (November 7, 2001): ***Yahoo! Inc., vs La LigueContre Le Racisme Et l'Antisemitisme a French association, et al***[236]

"This case is not about the moral acceptability of promoting the symbols or propaganda of Nazism. Most would agree that such acts are profoundly offensive. By any reasonable standard of morality, the Nazis were responsible for one of the worst displays of inhumanity in recorded history. This Court is acutely mindful of the emotional pain reminders of the Nazi era cause to Holocaust survivors and deeply respectful of the motivations of the French Republic in enacting the underlying statutes and of the defendant organizations in seeking relief under those statutes. Vigilance is the key to preventing atrocities such as the Holocaust from occurring again.

[235]Dr Gupta &Agarwal, Cyber Laws, Premier Publishing Company, Allahabad, 2010, at pg no 324
[236]*Yahoo! Inc, v La LigueContre Le Racisme Et l'Antisemitisme a French association, et al*145 FSupp 2d 1168, 1179 (N D Cal)[2001]

The Court concluded "that enforcement of the French order by a United States court would be inconsistent with the First Amendment, the factual question of whether Yahoo! possesses the technology to comply with the order is immaterial. Even assuming for purposes of the present motion that Yahoo! does possess such technology, compliance still would involve an impermissible restriction on speech.[237]

1.11 WHAT NEXT?

Undeterred by the verdict given by the District Court of Northern California a group called the Association Amicale des DiportisD'Auschwitz (AADA) filed a criminal case (February, 2002) against Yahoo! Inc. and its former CEO, Tim Koogle for allowing Nazi memorabilia to be sold through their websites thereby justifying war crimes against humanity, in the Tribunal Correctional de Paris.[238]

After the preliminary filing of documents, the trial date was set, January 7, 2003. Under French criminal law, acts committed outside of France by a non-French citizen, which in his home country would not be a violation of its local criminal law, may not be prosecuted before the French courts unless the acts involve crimes against humanity or certain special crimes, such as false declarations by foreigners in foreign Consulates or acts against the State (e.g. espionage or terrorism).

On February 11, 2003, the French criminal court dismissed all charges, holding that Yahoo! Inc. and its former CEO, Tim Koogle, never tried to "justify war crimes (or) crimes against humanity".

1.12 THE MESSAGE

Yahoo! case singularly demonstrates the conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of the US and France. In the civil case filed by LICRA, the French court aptly applied the private international law as it had a foreign element in the form of display and availability of objects (Nazi memorabilia) hosted by a US-based company (Yahoo! Inc.). This judicial competence (French Court) was well supported by the legislative jurisdiction in the form of an "offence against the collective

[237]Yahoo! Inc, a Delaware Corporation, Plaintiff-appellee
<https://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/>
[238]DrFarooq Ahmad, Cyber Law in India, New Era Law Publication, New Delhi, 2012, pg no 28

memory" (Articles 808 and 809 of the New Code of Civil Procedure) and Section R645-1 of the French Criminal Code, which prohibits the exhibition of Nazi propaganda and artifacts for sale. Similarly, the US Court's view that though "France has the sovereign right to regulate what speech is permissible in France, this Court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders" reflects both legislative and personal jurisdiction (of the US Court).

Also, it was held by the Italian Court of Cassation[239] that loading defamatory information onto a foreign server and displaying its contents on computer screens in Italy constitutes a single actusdelicti of defamation under Article 6 of Italy's Criminal Code, which defines the Code's scope of application as encompassing "all acts or omissions or even the effects of such action or omission which have occurred in whole or in part on Italian territory".

Expressed as a symbol of national sovereignty, the 'freedom of expression' has a different meaning in every nation-state. It is dependent on legislative and personal jurisdiction. Every nation-state has its version of 'freedom of expression'. Hence, it is too early to adopt the "Yahoo!" case as some sort of benchmark.

1.13 LET'S SUM UP

In this chapter, we have studied the essence of Yahoo! case, along with the issues brought before the court of law. We discussed the question that was posed before the experts and the opinion of the experts. Finally, we ended the discussion with the findings of the courts and the outcome of Yahoo!'s case.

1.14 FURTHER READING

- Freeman, R. & Wicks, Andrew &Werhane, Patricia & Mead, Jenny. (2008). Yahoo! And Customer Privacy (a). Darden Business Publishing Cases. 1. 10.1108/case.darden.2016.000356.
- Gautam, Shalini. (2016). Case Study-VERIZON'S YAHOO. The Case Centre.
- Yahoo! Shopping Auctions, Shopping Auctions Guidelines, at http://user. auctions.shopping.yahoo.com/html/guidelines.html (last visited Oct. 14, 2002).

[239] *Attorney General v Unidentified Person*, Judgment 4741, Nov. 17-Dec 27, [2000]

- Bellanger, P. (2011). From sovereignty in general to digital sovereignty in particular. In Les Echos.fr, 54(30). Retrieved from http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221137239/souverainete-general-et-souverainete-numeriq (Accessed 28 February 2012)
- Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. Security Dialogue, 43(1), 3-24.
- Choucri, N., & Clark, D. (2013). Who controls cyberspace? Bulletin of the Atomic Scientists, 69(5), 21-31.

1.15 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the main aim of Yahoo!?

It is an all-purpose portal providing services such as Internet search engine, email, an automated auction site, personal web page hostings, shopping services, chat rooms, and a listing of clubs that individuals can create or join.

2) What are the questions posed before the experts?

The expert opinion was sought, whether it is possible to:

a) Know the geographical origin and nationality of surfers wishing to access its auctions site.

b) Prevent French surfers or surfers connecting from French territory from perusing the description of Nazi objects posted for auction, and even more important to prevent them from bidding.

3) What was the outcome of Yahoo! case?

Yahoo! case singularly demonstrates the conflict between legislative jurisdiction (or national legislative competence) and personal jurisdiction (or judicial competence) of the US and France.

1.16 ACTIVITY

Explain the facts and the verdicts given by different courts in Yahoo!'s case, along with the outcome of the case? (800-1000 words)

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-949119-3-7

BAOU
Education for All

Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-102

E-Commerce, E-Governance and E-Contract

Post Graduate Diploma in Cyber Law (PGDCL)

2020

E-Commerce, E-Governance and E-Contract

Dr. Babasaheb Ambedkar Open University

E-Commerce, E-Governance and E-Contract

Course Writer

Dr. Peter Ladis F	Faculty, Chanakya Law University, Patna, Bihar
Mr. Kumar Gaurav	Faculty, Chanakya Law University, Patna, Bihar

Content Editors

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. June 2020

This publication is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) https://creativecommons.org/licenses/by-nc-sa/4.0/

ISBN: 978-81-949119-8-2

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

PGDCL-102

E-Commerce, E-Governance and E-Contract

Block-1: E-COMMERCE

UNIT-1 OVERVIEW OF E-COMMERCE 006

UNIT-2 HISTORICAL DEVELOPMENT AND REGULATORY FRAMEWORK OF E-COMMERCE 020

UNIT-3 SECURITY CHALLENGES AND FUTURE OF E-COMMERCE 032

UNIT-4 TAXING E-COMMERCE 047

Block-2: E-GOVERNANCE

UNIT-1 HISTORICAL DEVELOPMENT AND CONCEPT OF E-GOVERNANCE 059

UNIT-2 LEGAL ISSUES AND REGULATORY FRAMEWORK OF E-GOVERNANCE 072

UNIT-3 NATIONAL E-GOVERNANCE PLAN (NeGP) 088

UNIT-4 INTEGRATED AND STATE MISSION MODE PROJECTS 102

Block-3: E-CONTRACT

UNIT-1 OVERVIEW OF E-CONTRACT 118

UNIT-2 MAJOR ISSUES AND REGULATORY FRAMEWORK OF E-CONTRACTS 129

UNIT-3 COMPARATIVE ANALYSIS OF E-CONTRACT IN VARIOUS COUNTRIES 141

UNIT-4 EXERCISE OF JURISDICTION AND ISSUES RELATED THEREWITH 150

Block-4: INTERNATIONAL PERSPECTIVE

UNIT-1 IMPORTANCE OF INTERNATIONAL ORGANIZATION IN E-COMMERCE 161

UNIT-2 OVERVIEW OF ENTITIES AND NGO'S INVOLVED IN E-COMMERCE 173

UNIT-3 IMPLEMENTATION OF MODEL LAW AND DEVELOPMENT IN INDIA 186

UNIT-4 DARK WEB AND INTERNATIONAL CYBER LAWS 201

Block-1
E-Commerce

Unit 1: Overview of E-Commerce

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Salient features of E-commerce

1.4 Advantages of E-commerce

1.5 Disadvantages of E-commerce

1.6 Models in E-commerce

1.7 FDI in E-commerce

1.8 Inventory Model and FDI

1.9 Marketplace Model and FDI

1.10 Legal issues and solutions in E-commerce

1.11 Let's sum up

1.12 Further reading

1.13 Check your progress: Possible answers

1.14 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Models in e-commerce
- FDI in e-commerce
- Technical and Legal issues of E-Commerce

1.2 INTRODUCTION

The advent and growth of e-commerce in India brought some significant legal and regulatory challenges. Electronic commerce, commonly known as e-commerce or e-comm, is the platform

for buying and selling of products or services over electronic routes, such as the Internet and other computer networks. It involves sharing of business information, maintaining and conducting business transactions and relationships using a computer or a similar device connected to the telecommunication network. The traditional methods of communication channels like posts and telegraphs which once played a pivotal role in spreading commerce across the globe have now transmuted with the tremendous advancement of technology. E-commerce technologies have changed the framework and environment of business worldwide. Modern electronic commerce encompasses a wide range of technologies such as e-mail, mobile devices, telephones etc. It paves the way for a boundary-less virtual marketplace, without any geographical limitations, reaching global audiences. In the present era, E-commerce is considered a star of the Information Technology revolution and the Internet.

1.3 SALIENT FEATURES OF E-COMMERCE

1. Ubiquity

Internet / Web technology is omnipresent, and the outcome is known as *'Marketspace'*. A marketspace is a place extended beyond the traditional boundaries and removed from the temporal and geographic location. It is a method that saves transaction cost, and time, i.e., customer convenience is enhanced and shopping costs are reduced, unlike traditional commerce where one has to visit the market place physically.

2. Global Reach

The e-commerce transactions have crossed all the cultural and national boundaries across the globe. Marketspace includes potentially billions of consumers and millions of businesses worldwide compared to traditional commerce which couldn't cross national boundaries.

3. Universal Standards

E-commerce has become universal with the support of the Internet. They are shared by all the nations, as opposed to traditional technologies which differed from one nation to the other. For the merchants, market-entry cost remains constant all over the world, and it is lowered by

virtue of the internet. For the customers, the prices of products are lowered. The prices are uniform throughout the world and can be explored from any part of the world.

4. Richness

Information pertaining to any product can be acquired easily. Traditional markets and retail stores are able to provide prompt audio and visual information about the products. The messages are spread evenly and throughout the world i.e., complexity and the content of the message are the same.

5. Interactivity

E-commerce allows two-way communications between the merchant and the customer i.e., it can be used for both sending and receiving information from the internet using different websites.

6. Information Density

The information that is made available on the web is more accurate and reaches the person fast in a timely manner. The information is complete and is available to consumers, merchants and participants. This reduces information costs and raises quality. Communication costs drop dramatically while on the other hand, currency, accuracy and timeliness improve greatly. Information becomes ample, cheap and accurate.

7. Personalization / Customization

The advancement in technology in E-commerce allows personalization by targeting its marketing message to a specific person and adjusting a message based upon the person's name, interests and past purchases. The technology permits customization by changing the product according to the user's requirement. Due to information density, a lot of information about the customers and their requirements can be stored.

1.4 ADVANTAGES OF E-COMMERCE

- The messages and information reach across the globe in no time which makes the process effective and cheap for both suppliers and customers.

- The cost required to set up an office is very high compared to the cost of setting up a website which in turn can be integrated with fewer efforts.
- Newmarket segments can be explored with the use of the internet.
- An online store works 24 hours a day, 7 days a week, 365 days a year through an electronic data interchange system.
- Cost of order processing is reduced.
- Supply chain management is simpler, faster and cheaper with the use of e-commerce.
- Business can reach worldwide and there are high possibilities of establishing business partnerships.

1.5 DISADVANTAGES OF E-COMMERCE

- Electronic Data Interchange is expensive for small business entities.
- Security of internet is poor as virus invasion and hacker attacks can paralyze e-commerce. As a result of this, many companies and customers are harmed.
- Privacy of e-transactions is not guaranteed.
- The use of the Internet is only limited to the young and highly educated people. Elderly people are not prone to use the internet and hence cannot be customers for the internet-based business.
- E-commerce de-personalizes shopping.

1.6 MODELS IN E-COMMERCE

E-commerce models are of two kinds:-

a) Inventory based model

Inventory based model of e-commerce (Inventory Model) means an e-commerce activity where an inventory of goods and services is owned by an e-commerce entity and is sold to the consumers directly.[1]

b) Marketplace based model

[1]India's Foreign Investment Policy on E-commerce Retail: <https://corporate.cyrilamarchandblogs.com/2020/02/indias-foreign-investment-policy-on-e-commerce-retail/>

Marketplace based model of e-commerce involves an e-commerce entity providing an information technology platform on a digital and electronic network so as to act as a facilitator between the buyer and seller.

1.7 FDI IN E-COMMERCE

Foreign Direct Investment (FDI) in India is regulated under the Foreign Exchange Management Act, 1999 (FEMA). The Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry, Government of India enacts policy announcements on FDI through Press Notes and Press Releases which are notified by the Reserve Bank of India (RBI) as amendments to Foreign Exchange Management (Transfer or Issue of Security by Persons Resident Outside India) Regulations, 2000.[2]

The prevailing policy in India does not allow foreign investment in the business of selling via online platforms to consumers i.e., the current policy does not allow FDI in business-to-consumer (B2C) e-commerce activities, but 100% FDI is allowed in business-to-business (B2B) e-commerce and in the marketplace model under which the e-retailer does not sell directly to consumers, instead provides a platform to other sellers. US-based e-commerce corporations like Amazon and e-bay operate in India through the market place model.

The consolidated FDI Policy issued by the DIPP (FDI Policy) lays down two entry routes for investment:-

- Automatic Route where foreign investments do not require prior approval of the government and
- Government / Approval route where prior approval of the Government of India through Foreign Investment Promotion Board (FIPB) is required.

1.8 INVENTORY MODEL AND FDI

[2]Foreign Direct Investment Fdi Policy - 877 Words | Bartleby <https://www.bartleby.com/essay/Foreign-Direct-Investment-Fdi-Policy-FKEEY63LDE7W>

Inventory Model is the Business-to-Consumer (B2C) model of e-commerce and FDI in such model is strictly prohibited.[3] However, Press Note No. 12 of 2015 clarified that subject to the Consolidated FDI Policy with regard to sectors and provision of services through e-commerce, the Inventory Model will be under the automated route.[4]

Press Note No. 12 of 2015 (Press Note 12) provided that certain manufacturers engaged in single-brand retail would be entitled to receive FDI upon certain conditions, such as follows[5]:-

a) An Indian manufacturer who is permitted to sell its own branded product through wholesale retail e-commerce platforms.
b) An Indian manufacturer, who is an investee company, manufacturing in India, in terms of value, at least 70% of its product in house, and sources, at most 30% from other Indian manufacturers.
c) A single brand retail trading entity operating through brick and mortar stores.

Additional Conditions as mentioned under Press Note 12

- The product should be sold under the same brand internationally.
- **'Single Brand'** product retail trading would cover only products which are branded during manufacture.[6] Therefore, branding as a separate activity may not be considered as branding for single-brand.
- Non-resident entities whether as owners of a brand or otherwise shall be authorized to undertake single-brand retail trading through an agreement with the brand owner, thereby entitling the non-resident entity to undertake single brand product retail in India.
- FDI proposals of more than 51% would require 30% of the value of goods purchased to be from within India and preferably from MSMEs, village and cottage industries, artisans and craftsmen.

1.9 MARKETPLACE MODEL AND FDI

[3]Para 2.2. (ii) of the Press Note
[4]Para 3 of the Press Note
[5]Research and Articles - Nishith Desai Associates
<http://www.nishithdesai.com/information/research-and-articles/nda-hotline/nda-hotline-single-view/article/clarity-to-ambiguities-in-fdi-in-e-commerce-will-it-reduce-litigation.html>
[6]Para 2.2.25: "Manufacture", with its grammatical variations, means a change in a non-living physical object or article or thing– a) resulting in transformation of the object or article or thing into a new and distinct object or article or thing having a different name, character and use; or b) bringing into existence of a new and distinct object or article or thing with a different chemical composition or integral structure

The Department of Industrial Policy and Promotion (DIPP) had established certain clarifications in the Press note pertaining to the Marketplace model. They are as follows:-

- Marketplace models entities have been permitted to enter transactions with sellers registered on its platform on Business-to-Business (B2B) basis. However, each seller or its group companies would not be allowed to sell more than 25% of the total sales of the Marketplace Model entity. On the other hand, this amendment affects the business of certain e-commerce entities where the majority of sales are made by one retail entity.
- Marketplace Models have been allowed to provide support services to sellers in respect of warehousing, logistics, order fulfilment, call centre, payment collection and other services. This paves way for e-commerce entities to have in-house support services instead of reaching out for third-party service providers.
- For any warrantee or guarantee or return of goods and services sold under this model, the seller will be held responsible and not the e-commerce entity i.e., responsibility for the delivery of goods to the customers and ensuring customer satisfaction would be that of the seller and not the intermediary entity. Added to that, liability under consumer protection laws would be on the sellers and not the e-commerce entities.
- Under this model, e-commerce entities should not exercise ownership over the inventory i.e., goods purported to be sold, otherwise, such ownership over the inventory will render the business into inventory model.
- E-commerce entities cannot 'directly or indirectly influence the sale price of goods or services' and are obligated to maintain a uniform level.

1.10 LEGAL ISSUES AND SOLUTIONS IN E-COMMERCE

a) Authentication and Identification

Although the Internet eliminates the need of physical contact, the transactions that take place, especially consumer-related transactions occur between parties who have no pre-existing relationship. This raises a lot of issues pertaining to persons' identities as well as the

authenticity thereof. Some of the issues that need to be taken into consideration by companies are:-

- **Digital Signatures to be used as authentication tools**

  The Information Technology Act stipulates that digital signatures may be considered as one of the methods used to determine the authority and legitimacy of the person to authenticate an electronic record. The digital signature must follow the Public Key Infrastructure (PKI).[7] This acts as a limitation on the use of any other technology for the purpose of authentication. If the Indian companies commence using other technologies for the authentication process which are not legalized, it could be said that there has been no authentication at all.[8] The IT Act provides that an electronic signature shall be deemed to be a secure electronic signature if:

  - The signature creation data, at the time of affixing the signature, was under the exclusive control of the signatory and no other party;[9] and
  - The signature creation data was stored and affixed in such exclusive manner as prescribed under the IT Act.

- **Identity Theft and Impersonation**

  The IT Act provides that the identity of a person shall be deemed to have been stolen when any unique identification of a person (such as electronic signature or password) is fraudulently or dishonestly used. The Act prescribes a penalty of imprisonment of upto 3 years and fine upto 1 lakh rupees.[10]Added to that, if any person cheats by impersonation by means of any communication device or computer resource, he shall be punished with imprisonment of upto 3 years and fine upto 1 lakh rupees.[11]

  The Indian Penal Code provides that any person who cheats by personation shall be punishable with imprisonment of upto 3 years and / or fine.[12]

[7] Section 3 of IT Act
[8]LEGAL ISSUES IN eCOMMERCE - Nishith Desai Associates <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Legal_issues_in_eCommerce.pdf>
[9]E-Commerce in India - Nishith Desai Associates | 1pdf.net <https://1pdf.net/e-commerce-in-india-nishith-desai-associates_5850c203e12e89cd355094cd>
[10] Section 66-C of the IT Act
[11] Section 66-D of the IT Act
[12] Section 419 – Punishment for cheating by personation

b) ***Security of Systems***

Security over the Internet is of immense importance in the present era. Since e-commerce companies manage their sensitive information (including Sensitive Personal Data or Information) on their servers, the companies must ensure that they have adequate security measures to safeguard their systems from unauthorized intrusions. A company could face security threats internally as well as externally. Security can be maintained by making use of various security tools such as encryption, firewalls, access codes/passwords, virus scans and biometrics.

c) ***Privacy and Data Protection***

An important consideration for every e-commerce website is to maintain the privacy of its users. In an e-commerce platform, it is quite difficult to complete any online transactions without making use of some form of personal information of the users such as details with regard to their identity and financial information. With the help of innovative technologies and lack of secure systems, it would be easy to obtain personal and confidential information about individuals and organizations.[13] Apart from collecting the primary data from the users, e-commerce platforms also collect a variety of other indirect information such as users' personal choices and preferences and patterns of search. One of the important consideration for every e-commerce platform is to maintain the privacy of its users.

Historically, the concept of privacy and data protection were not addressed in any of the Indian legislations. However, the Supreme Court of India in the cases of ***Kharak Singh Vs State of UP***[14]and ***People's Union of Civil Liberties Vs Union of India***[15]recognized the 'right to privacy' as a subset of Article 21 of Constitution of India i.e., right to life and personal liberty.

The Indian Constitution upholds the right to privacy as a fundamental right of every citizen,[16] the right is exercisable only against a state action. The IT Act addresses the issue of safeguarding privacy rights only from Government actions.[17] Under the IT Act, if the privacy

[13]Legal Issues in e-Commerce - UNECE Homepage <https://www.unece.org/fileadmin/DAM/cefact/cf_forums/2018_China/eCommerce_Bio-PPT/PPT_10_Khan.pdf>

[14]*Kharak Singh v State of UP* AIR [1963] SC 1295

[15]*People's Union of Civil Liberties v Union of India*[1997] (1) SCC 318

[16]Article 19 (1) (a) and Article 21 of the Constitution. Refer to *Unni Krishnan, J P* v *State of AP*[1993] 1 SCC 645

[17]Section 69 and Section 72 of the Information Technology Act, 2000

of a person is deemed to be violated, a punishment of imprisonment of upto 3 years and/or fine upto 2 lakh rupees shall be imposed.

In 2011, Section 43A of the IT Act titled *"Reasonable practices and procedures and sensitive personal data or information Rules, 2011"* provided a framework for the protection of data in India which covered two categories of information under the Act. They are:-

- **Personal Information (PI)** which is defined as any information that relates to a natural person, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- **Sensitive Personal Data or Information (SPDI)** which means that such personal information of a person which consists of
    i. Password
    ii. Financial information such as bank account or credit card or debit card or other payment instrument details
    iii. Physical, physiological and mental health condition
    iv. Sexual orientation
    v. Medical records and history
    vi. Biometric information

The IT Act lays down penalties for wrongful disclosure of personal information by way of imprisonment upto 3 years and/or a fine upto 5 lakh rupees.

d) ***Intellectual Property Rights***

The Internet is a boundless and unregulated medium and therefore the protection of Intellectual Property Rights (IPR) is a challenge and a growing concern amongst most e-businesses. The efficacy of Indian laws in safeguarding the rights in e-commerce is not an easy task. Some of the significant issues that arise with regard to protecting IPRs in e-commerce are as follows:-

- **Determining the subject matter of protection**

  With the advent of new technologies, new forms of IPRs are evolving and the challenge for any business would be in determining how best its intellectual assets can be protected.
- **Designing a Platform / Content Creation through a Third Party**

  Often e-commerce entities outsource the job of designing websites/creation of content to third party contractors. This creates an issue with regards to who would own the IP in the

design and functionality (software underlying the website) of the website and in the content. Some important elements which need to be taken into consideration are as follows:-

i. A written agreement that clearly determines the ownership of the IP including clauses on term, territory and the nature of the right.
ii. If any third party is used by the contractors, it is important to understand the chain of title with respect to such third-party IP and whether appropriate permissions have been acquired from such third parties.

- **Use of Third Party Content on website**

  Not all content available on the public domain can be used for free without prior permission of the owners of such content. The content could range from information to logos of third parties. The IP of the said content is owned by a third party and the e-commerce business has to obtain the requisite approvals.

- **Prevention of unauthorized hyperlinking and meta-tagging**

  E-commerce companies often have to deal with hyperlinking, deep linking,[18]framing[19] and meta-tagging[20] issues in order to achieve their marketing goals. The Judiciary in many countries has dealt with issues concerning infringement of IPRs arising from hyperlinking and meta-tagging activities. They have held that hyperlinking, especially deep linking may constitute copyright infringement; and on the other hand, meta-tagging may constitute trademark infringement. The Indian Courts have not yet dealt with these issues in detail.

  The US courts have held in cases of ***Ticketmaster Vs Tickets.com***[21]and ***Batesville Serv. Inc. Vs Funeral Depot Inc.***[22]that linking to another website could constitute copyright infringement. Furthermore, in the cases of ***Playboy Enterprises Inc. Vs Calvin Designer***

[18]Hyperlink is a reference to a webpage or document on the Internet and deep hyperlink links to a specific interior page or paragraph inside a websitesurpassing the homepage
[19]Framing is the juxtaposition of two separate web pages within the same page
[20]Metatags are HTML codes that are intended to describe the contents of a web page but do not appear on the web page
[21]*Ticketmaster v Tickets.com*CV 97-3055 RAP (C D Cal, filed April 28, 1997)
[22]*Batesville ServInc v Funeral Depot Inc*No 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S D Ind Nov 10, 2004)

Lab[23]and***Nat'l Envirotech Group L.L.C., Institution Technologies Inc. Vs Nat'l Envirotech Group L.L.C***[24]**it was** held that using competitors' trademarks in the meta tags would be an infringement of such trademarks. The UK courts have also asserted the same view in the case of ***Roadtech Computer Systems VsMandata Ltd***[25]and ***Reed Executive plc and another Vs Reed Business Information and others.***[26]

- ***Domain Names***

A company that commences e-commerce activities would at first have to get a registration of its domain name which must not be similar to some other domain names or some existing trademark of a third party. If any company's domain name is found to be similar to that of another, then the company could be held liable for cybersquatting. Indian Courts have been proactive in granting orders against the use of infringing domain names.[27] In the case of ***Satyam Infoway Ltd. VsSifynet Solutions Pvt. Ltd.,***[28]the Supreme Court held that 'a domain name may pertain to the provision of services within the meaning of Section 2(z) of the Trade Marks Act, 1999'.

e) ***Taxation***

Taxation of e-commerce transactions has raised several issues. Tax authorities all over the world are examining the tax implications of e-commerce transactions and resolving mechanisms to tax such transactions.[29] In India, the High Powered Committee (HPC) constituted by the Central Board of Direct Taxes, submitted its report in September 2001. The said report envisaged upon the need for introducing a separate tax regime for e-commerce transactions. Based on the Principle of 'Neutrality', the HPC maintained that the existing laws are sufficient to tax e-commerce transactions and held that there is no need for a separate regime for the taxation of e-commerce transactions.

---

[23]*Playboy Enterprises Inc v Calvin Designer Lab*[1997] U S Dist Lexis 14345 (D Cal Sept 8, 1997)

[24]*Nat'l Envirotech Group LL C, Institution Technologies Inc v Nat'l Envirotech Group L LC* Civil Action 97-2064 (E D La)

[25]*Roadtech Computer Systems vMandata Ltd* [2000] ETMR 970

[26]*Reed Executive plc and another v Reed Business Information and others* [2004] EWCA Civ 159

[27]Some of the cases in which injunctions against the use of conflicting domain names have been granted are: Yahoo Inc vAakashArora&Anr*AIR*[*2000]Bom 27*; Rediff Communication v Cyberbooth&*Anr[1999] PTC (19) 201*and Satyam Infoway Ltd v Sifynet Solutions Pvt Ltd *AIR [2004] SC3540*

[28]*Satyam Infoway Ltd vSifynet Solutions Pvt Ltd* AIR [2004] SC 3540

[29]An overview on e-commerce transactions - CAclubindia <https://www.caclubindia.com/articles/an-overview-on-e-commerce-transactions-24119.asp>

1.11 LET'S SUM UP

In this chapter, we have studied the meaning of e-commerce, its salient features, advantages and disadvantage and its models. We also studied how FDI plays a vital role in e-commerce. Finally, we ended the discussion with the legal issues and solutions in e-commerce.

1.12 FURTHER READING

- The eComTaxpert Group, "Taxation of Electronic Commerce in India", [2002] Asia-Pacific Tax Bulletin July/August 241
- The law of E- commerce: E- contracts, E-business by Dr. Abdullah M. Alghamdi- Published my Author house, Bloomigton. 1-4.
- Law relating to e- commerce: international and national scenario with special reference to India Dr.Jyoti Rattan. (IJSSEI) Volume//01//Issue//02//August 2015 Dr.Jyoti Rattan(www.isij.in)

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is e-commerce?

A. E-commerce is the method by which products and services are bought and sold by electronic means using the internet and mobile applications.

2. What are the advantages of e-commerce?

A. The advantages of e-commerce are as follows:

- Messages and information reach across the globe in no time which makes the process effective and cheap for both suppliers and customers.
- The cost required to set up an office is very high compared to the cost of setting up a website which in turn can be integrated with fewer efforts.
- Newmarket segments can be explored with the use of the internet.
- An online store works 24 hours a day, 7 days a week, 365 days a year through an electronic data interchange system.
- Cost of order processing is reduced.

- Supply chain management is simpler, faster and cheaper with the use of e-commerce
- Businesses can reach worldwide and there are high possibilities of establishing business partnerships

3. What are the disadvantages of e-commerce?

A. The disadvantages of e-commerce are as follows:

- Electronic Data Interchange is expensive for small business entities.
- Security of internet is poor as virus invasion and hacker attacks can paralyze e-commerce. As a result of this, many companies and customers are harmed.
- Privacy of e-transactions is not guaranteed.
- The use of the Internet is only limited to the young and highly educated people. Elderly people are not prone to use the internet and hence cannot be customers for the internet-based business.
- E-commerce de-personalizes shopping

4. What are the various models and salient features of e-commerce?

A. The various models of e-commerce are inventory-based model and marketplace-based model.

The salient features of e-commerce involve ubiquity, global reach, universal standards, richness, interactivity, information density and personalisation or customization.

5. Mention the kinds of legal issues involved with e-commerce?

A. Legal issues involved with e-commerce inter alia involve authentication and identification of users, security of systems engaged in the exploration of cyberspace, protection of privacy and data, protection of intellectual property rights.

1.14 ACTIVITY

Demonstrate E-Commerce and discuss its objectives, advantages and challenges? (800 words)

Unit 2: Historical Development and Regulatory Framework of E-Commerce

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Historical Development and Concept of E-Commerce

1.4 Conceptual Framework

1.5 Types of e-commerce

1.6 Regulatory framework of E-Commerce under I.T. Act, 2000

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Historical and emergence of e-commerce
- Types of e-commerce
- Regulatory framework of e-commerce

1.2 INTRODUCTION

Electronic commerce, a new means of carrying out business transactions through electronic means in general, and through Internet environment in particular, has been proving its potential benefits and effective contribution to the socio-economic growth. As an essential part of the "digital economy", electronic commerce plays the role as the key for us to open our door to the 21st century, the new era of the knowledge-based economy. In the context of electronic commerce, there is a need to define the framework of e-commerce.[30]

[30] E-commerce: An Introduction, <http://cyber.law.harvard.edu/olds/ecommerce/setuptext.html>

'Electronic commerce is sharing business information, maintaining business relationships and conducting business transactions by means of telecommunications networks'. E-Commerce is one of the most important facets of the Internet to have emerged in recent times. E-commerce or electronic commerce involves carrying out business over the Internet with the assistance of computers, which are linked to each other forming a network. To be specific e-commerce would be buying and selling of goods and services and transfer of funds through digital communications.

Today, e-commerce is a major economic force driving growth for developed as well as developing countries. The exponential growth of Internet use and online purchases globally combined with the relatively low cost of Internet marketing is enabling large companies as well as small and medium-sized enterprises (SMEs) to expand their market overseas through e-commerce.

As per the Economic Survey 2017-18, the electronic commerce (e-commerce) market in India is estimated at USD 33 billion, with a 19.1 percent growth rate in 2016-17.[31] As per the National Association of Software and Services Companies (NASSCOM) Strategic Review 2018, in the Information Technology and Business Process Management (IT-BPM) sector in India, the Indian e-commerce market was USD 33 billion in 2017-18 and reached USD 38.5 billion, growing at a rate of about 17% in the financial year 2018-19.

1.3 HISTORICAL DEVELOPMENT AND CONCEPT OF E-COMMERCE

The development of the World Wide Web during the early 1990's dramatically changed the use of the internet. The expansion of the web, and along with it the web browser opened the internet to anyone with basic computer experience and an online connection. As online activity increased, companies quickly saw the internet's marketing potential. Subsequently, there was a rush to take products and services into this expanding electronic realm and to redefine business itself.[32]E- commerce, in full electronic commerce, maintaining relationships and conducting a business transaction that induces selling information, services, and goods by means of computer

[31]"India : E-Commerce Business." MENA Report, Albawaba (London) Ltd, Feb 2019
[32]Electronic Commerce
<http://afreidooni.blogfa.com/post/46>

telecommunications networks.[33] Although in the vernacular e-commerce usually refers only to the trading of goods and services over the internet, broader economic activity included. E-commerce consists of business to consumer and business to business commerce as well as internal organizational transactions that support those activities. E-commerce originated in a standard for the exchange of business documents, such as orders or invoices, between suppliers and their business customers. Those origins date to 1948-49, Berlin blockade and airlift with a system of ordering goods primarily via telex. Various industries elaborated upon that system in the ensuing decades before the first general standard was published in 1975. The resulting computer to computers electronic data interchange (EDI) standard is flexible enough to handle most simple electronic business Transactions with the wide adoption of the internet and the introduction of the world wide web in 1991 and of the first browser for accessing it in 1993, most E-commerce sifted to the Internet. More recently, with the global spread of smartphone and the accessibility of fast broadband connections to the Internet, much E-commerce moved to mobile devices, which also included tablets, laptops, and wearable products such as watches. Today the number of internet users in the world is close to 3 Billion. Out of this India have a total of 259.14 Million Internet and broadband subscribers.[34] This penetration of Internet coupled with the increasing confidence of the internet user to purchase online has led to enormous growth in the E-commerce space, with an increasing number of customers registering on E-commerce web sites and purchasing products through the use of mobile phones. It is not surprising therefore that India in a prime position for the growth and development of the E-commerce sector. In particular, E-commerce present one of the greatest opportunities in the retail sector since it provides a dramatic change from Brick and mortar establishment to virtual shops which could operate for a fraction of the cost. E-commerce has deeply affected everyday life and how business and governments operate. Commerce is conducted in electronic market places and in the supply chains working on the internet web.[35] Consumer-oriented market places Include large E-mails (such as Amazon) consumer to consumer auction platforms (eBay, for examples) multi-channel retailers and many millions of E-retailers. Massive business to business market places has been created by Alibaba and other companies. Social networks sites, such as Facebook

[33]Chauhan, Abha (2013), "Evolution and Development of Cyber Law – A Study with Special Reference to India," Social Science Research Network

[34]BaharulIsalm, K M (2008), "E-commerce: Laws and Cyber Crimes," academia.edu

[35] 'Trends In India's e-Commerce Market': Report provided by Forrestor Research for ASSOCAM's 2nd National Conference on e-Commerce 2012

undergird a great verity of individual relationships and are the sites of so-called social commerce, driven by the opinions and reviews shared by the participants as the electronic word of mouth. The web is also an interactive medium of human communication that supplements and often replaces traditional media. The hypermedia nature of the web with the interlinking of multimedia content available on globally distributed sites, enables the creation of new types of media products, Often offered free of charge. Those new media include Blogs, video aggregators (Such as YouTube), Social media and customized electronic newspapers. As with all media, this aspect of the web leads to its use in marketing. Web advertising ranges from the display ads on web sites to Keyword ads shown to information seekers using search engines, such as Google.

1.4 CONCEPTUAL FRAMEWORK

Simply put, E-**commerce is buying and selling on electronic networks, predominantly the Internet. This could i**nvolve a trade of tangible goods/services similar to traditional commerce, or intangible items like music, information and involving digital transfer etc.

The word commerce is the basic concept for electronic commerce, pertaining to buying and selling of goods while 'commercial' denotes business practice and activities intended to make profits. Electronic commerce, like any other business, deals with the exchange of money for soft or hard goods and services.

Kalakota and Whintons in 1997 defined the term E-commerce from different perspectives. These perspectives are:

- Communication
- Business Process
- Service
- Online

COMMUNICATION PERSPECTIVE:

According to this perspective, E-commerce is the delivery of information, product/services or payments over telecommunication channels, computer networks or any other electronic mode of communication.

BUSINESS PROCESS PERSPECTIVE:

This says that E-commerce is the application of technology towards the automation of business transactions and workflow.

SERVICE PERSPECTIVE:

E-commerce is defined as a tool that addresses the desire of firms, consumers and management to cut service cost while improving the quality of goods/services and increasing the speed of service delivery.

ONLINE PERSPECTIVE:

E-commerce provides the capability of buying and selling products and information on the internet and other online services.

Electronic Commerce (e-commerce) is an electronic business. It's using the power of computers, the Internet and shared software to send and receive product specifications and drawings; bids, purchase orders and invoices;[36] and any other type of data that needs to be communicated to customers, suppliers, employees or the public. E-commerce is the new, profitable way to conduct business which goes beyond the simple movement of information and expands electronic transactions from point-of-sale requirements, determination and production scheduling, right through to invoicing, payment and receipt. E-commerce uses key standards and technologies including Electronic Data Interchange (EDI), Technical Data Interchange (TDI), Hypertext Markup Language (HTML), Extensible Mark-up Language (XML), and the Standard for Exchange of Product model data (STEP). E-commerce is made possible through the expanded technologies of the Internet, the World Wide Web, and Value-Added Networks.

The Organization for Economic Cooperation and Development (OECD) defines electronic commerce as a new way of conducting business, qualifying it as business occurring over networks which use nonproprietary protocols that are established through an open standard-setting process such as the Internet.[37] This definition distinguishes it from the earlier EDI type proprietary based networks or Intranets that were not based on an open (and, therefore, not cost-effective information infrastructure) like the Internet.[38] In the WTO Work Programme on Electronic Commerce, it is understood to mean the production, distribution, marketing, sale or

[36]Web and Value-Added Networks Essay - Lesson Plan Essay<https://larochelleairport.net/what-is-electronic-commerce-essay-2/>

[37]Electronic Commerce: Issues of Policy and Strategy for India <https://icrier.org/pdf/WP-86.pdf>

[38]E-COMMERCE AND RETAIL BUSINESS IN NIGERIA: CHALLENGES <https://nairaproject.com/m/projects/1190.html>

delivery of goods and services by electronic means. A commercial transaction can be divided into three main stages: the advertising and searching stage, the ordering and payment stage and the delivery stage. Any or all of these may be carried out electronically and may, therefore, be covered by the concept of 'electronic commerce'

The World Trade Organization (WTO) distinguishes six main instruments of electronic commerce:

- The Telephone,
- The Fax,
- Television,
- Electronic payment and money transfer systems,
- Electronic Data Interchange, and
- The Internet

Though the telephone, fax, TV and EDI have been in existence for some time when people talk of E-commerce, they usually refer to Internet Business, wherein goods or services are traded on the net.

1.5 TYPES OF E-COMMERCE

One way of classifying E-Commerce is based on parties involved in the transaction. Major types are mentioned below:[39]

- Business to Business (B2B)
- Business to Customers (B2C)
- Consumer-to-Consumer (C2C)
- Government to Business (G2B)
- Government to Citizens (G2C)

[39]Types of E-Commerce Models | Eyerys <https://www.eyerys.com/articles/types-e-commerce-models>

Business to Business: On the Internet, B2B (business-to-business), also known as e-biz and is defined as the exchange of products, services, or information between businesses such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.

Business to Consumer:A transaction that occurs between a company and a consumer. The term may also describe a company that provides goods or services for consumers.

Consumer to Consumer: Consumer-to-consumer (C2C) electronic commerce involves the electronically facilitated transactions between consumers through some third party. A common example is an online auction, in which a consumer posts an item for sale and other consumers bid to purchase it; the third party generally charges a flat fee or commission.

Government-to-Business(G2B):is a business model that refers to the government providing services or information to business organization. The government uses the B2G model website to approach business organizations. Such websites support auctions, tenders and application submission functionalities e.g. government procurement, electronic auctions, sending filled-out electronic forms (e.g. tax forms, social insurance forms).

Government to Citizen (G2C): is a term that refers to the relationships between organizations (subjects) of public administration and a citizen(s). The designation can be used for any relationship between the subject of public administration and the citizen, most often it is used as one of the basic relationship within e-Government models. The initiative comes from a federal organization (public administration) and citizens are the target group.

Another way of classifying E-Commerce is based on whether the Internet is used or other electronic devices are used for transactions. On this basis, we can classify them as (a) Non-Internet Based E-Commerce, and (b) Internet-Based E-Commerce.

Non-Internet Based E-Commerce:

There are many electronic devices, other than the Internet, which are used for the purpose of E-Commerce. For example (i) Bar-Code Machines, (ii) Vending Machines, (iii) Telephone & Telegraphs (iv) Fax (v) Television (vi) Standalone Computers (vii) Computer Network etc. Transactions made through the devices mentioned here are easy to understand except the use of Computer Network for Electronic Data Interchange (EDI). A discussion on EDI follows.

Electronic Data Interchange (EDI) - This is a business-to-business (B2B) type of E-Commerce. EDI is the computer-to-computer exchange of structured business information in standard electronic format. Information stored in one computer is translated by software programs into standard EDI format for transmission to one or more trading partners. Trading partner's computer, in turn, translates the information using software programs into a form they can understand. There is no human involvement in the processing of the information. EDI was developed in the 1960s. However only in the 1980s, a wide range of industries started using this technique.[40]

Organizations adopting JIT (Just in Time) purchasing, maybe much benefited if they adopt EDI. With the help of EDI, the supplier constantly gets information onthe stock position of the customer(s) online. On the basis of such information, the supplier can supply goods just in time. Let us suppose that a chicken farm has many outlets in a city, which sells varieties of chicken-based products. If the main office has a computer network with EDI facility with its outlets, it can easily monitor the stock position of the outlets. Whenever the stock position of a particular item in an outlet reaches reorder level, the main office computer will automatically initiate the reorder process. Thus it reduces time and expense of paperwork.[41]

Besides this, EDI is also used in international trade, electronic fund transfer (EFT) between supplier and customer via banker, insurance claim settlement etc. If properly used, EDI can save a substantial amount of cost involved in transaction processing.

Supply Chain Management (SCM) -As a part ofinternal E-commerce,Supply Chain Management is a landmark concept in inventory management. JIT inventory management is no doubt beneficial but still, it is only a part of the overall Supply Chain Management. On the other hand, SCM is an integrated approach which involves- supplier management, inventory management, distribution management and payment management. SCM considers that instead of treating these as separate functions, a holistic view is needed. Organizations are experiencing that if they have to respond to the needs of the fast-changing world; cross-function integration

[40]Yazdanifard, AsscProf DrRashad&Baruani, Baome&Mohseni, Shahriar (2012) Review of Electronic Data Interchange in Business to Business E-Commerce in a Competitive Global Market. RNIS: Research Notes in Information Science. 9. 48-53. 10.4156/rnis.vol9.issue0.6

[41] Andersen, Kim Normann&Juul, Niels Christian &Bj rn-Andersen, Niels& Bunker, Deborah. (2000). Electronic Commerce and Document Interchange: EDI Applications in Denmark. Copenhagen Business School, Department of Informatics, Working Papers

and use of information & communication technology is a must. All the functions in SCM are done electronically. SCM software solutions are also available in the market.

Internet-Based E-Commerce (I-Commerce):

By Internet Commerce, we mean the use of the global Internet and World Wide Web (WWW) for commerce. With the advent of Internet & Website (World Wide Web), is the all-pervasive communication tools, the scope of E-Commerce has increased manifold. At present, it is the most powerful *distribution channel* amongst all the channels. For these reasons, the term I-Commerce has become synonymous with the term E-Commerce. In the forthcoming paragraphs, we will use these two terms alternatively. In this context a basic idea about E-Commerce website is essential.

1.6 REGULATORY FRAMEWORK OF E-COMMERCE UNDER I.T. ACT, 2000

UNCITRAL MODEL LAW ON E-COMMERCE

UNCITRAL is the United Nations Commission on International Trade Law. Established by the United Nations in 1966 to harmonize the law of international trade, it is a core legal body of the United Nations system that works to create accessible, predictable and unified commercial laws. UNCITRAL created a Model Law on Electronic Commerce in 1996 to enhance the use of paperless communication.[42] In 2001, it created a Model Law on Electronic Signatures. Future electronic commerce work will focus on: electronic contracting, with a view to creating a draft convention; online dispute settlement; dematerialization of documents of title; and a convention to remove legal barriers to the development of electronic commerce in international trade instruments.[43]

THE INFORMATION TECHNOLOGY ACT, 2000 AND E-COMMERCE

[42]Luca Castellani, UNCITRAL Legislative Standards On Electronic Communications And Electronic Signatures: <An Introduction itu.int/dms_pub/itu-t/oth/15/08/T15080000020001PDFE.pdf>

[43] UNICTRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 *bis* as adopted in 1998, United Nations, New York, 1999, <https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf>

In India E-commerce falls within the purview of the Information technology Act, 2000. It legally recognizes all correspondence by electronic mail, the information in an electronic form with an electronic signature. The electronic is certified by the controller. It also recognizes application and approval done in electronic format for niceness, permits and at her documents pertaining to Government department. In addition, it also makes hacking download, copy, extract, damage of electronic files data liable for punishment.[44]

The Information Technology Act 2000 is based on the Model Law on E-commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and pioneering e-commerce enabling legislations such as the Utah Digital Signatures Act, 1995; the Singapore Electronic Transactions Act, 1999 and the Malaysian Electronic Signatures Act. The main objective behind the introduction of IT Act, 2000 is to encourage the environment in which the laws are simple and transparent and in which the advantages of e-commerce can be tapped.

The Act aims to provide legal recognition for the transactions carried out by the means of electronic data interchange and other means of communications, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper-based methods of the communication and storage of information, to facilitate electronic filing of document with the government agencies. The Act comprises of the three significant aspects of e-commerce:

- Legal recognition of electronic records and communications- contractual framework, evidentiary aspects, digital signatures as the method of authentication, rules for determining time and place of dispatch and receipt of electronic records.
- Regulation of Certification Authorities- appointment of a Controller of CAs, the grant of license to CAs, duties vis-à-vis subscribers of digital signature certificates, recognition of foreign CAs.
- Cyber contraventions- civil and criminal violations, penalties, the establishment of the Adjudicating Authority and the Cyber Regulatory Appellate Tribunals.[45]

[44] Gandhi, Sunil. (2006). E-COMMERCE AND INFORMATION TECHNOLOGY ACT, 2000

[45]Basu, Subhajit& Jones, Richard (2003) E-commerce and the law: A review of India's Information Technology Act, 2000 Contemporary South Asia 12. 7-24. 10.1080/0958493032000123344

As the Act establishes the legal validity and enforceability of the digital signature and electronic records as well as the secure digital signatures and secure electronic records, it will enable the growth of e-commerce in India, because the secure computer-based signatures will:

- Minimize the incidence of electronic forgeries.
- Enable and foster authentication of computerized communications.
- Facilitating commerce by means of electronic communications.

Further, electronic filing of records and retention of information in electronic formats, enabled by the IT Act, 2000 will help in saving costs, time and manpower for the corporate. By virtue of the recognition given to the electronic records, electronic documents and electronic signature, consequential amendments have been made in some existing laws. The Act amends the Indian Panel Code, 1860, the Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, and for the matters connected therewith or incidental thereto. The main purpose of these amendments is to address the related issues of electronic commerce, electronic crimes and evidence, and to enable further regulation as regards electronic fund transfer.

1.7 LET'S SUM UP

In this chapter, we have studied the historical development and conceptual framework of e-commerce. We also studied the types of e-commerce along with the regulatory framework under the Information Technology Act, 2000 in the end.

1.8 FURTHER READING

- Singh, Taranjeet. (2016). E-Commerce Scenario in India. 3. 16-19.
- Hazelton, Bill, 'History of E-Commerce,' Spirecast, August 19, 2009.
- Mitra (2013) "E-Commerce in India-A Review" Journal of Marketing, Financial Services & Management Research International, Vol.2,No.02,Kolkata,February 2013,pp 126-132.
- Rajasekar and Agarwal (2016) "A study of Impact of India-Commerce on India's Commerce" Indian Journal of Development and Research, Vol. 6, Issue 03.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the different perspectives of e-commerce?**
    - Communication
    - Business Process
    - Service
    - Online
2. **What are the different types of e-commerce?**
    - Business to Business (B2B)
    - Business to Customers (B2C)
    - Consumer-to-Consumer (C2C)
    - Government to Business (G2B)
    - Government to Citizens (G2C)
3. **What is EDI?**

EDI is the computer-to-computer exchange of structured business information in standard electronic format. Information stored in one computer is translated by software programs into standard EDI format for transmission to one or more trading partners.

4. **When did UNCITRAL create a Model Law on e-commerce?**

UNCITRAL created a Model Law on Electronic Commerce in 1996 to enhance the use of paperless communication.

1.10 ACTIVITY

Elucidate the different types of Internet and Non-Internet based E-Commerce along with the regulatory framework under the I.T. Act, 2000? (1000 words)

Unit 3: Security Challenges and Future of E-Commerce

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Legal Issues involved in E-Commerce

1.3 Security Challenges of E-Commerce

1.4 Best Practices to Combat E-Commerce Security Threats

1.5 Issues and Challenges in the newly drafted E-Commerce Policy Bill of India

1.6 Future of E-Commerce

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through chapter, you will be able to understand:

- Legal issues and Security challenges
- Issues and challenges in the new bill
- Future of E-Commerce

1.2 LEGAL ISSUES INVOLVED IN E-COMMERCE

With the advanced and increased use of online media, online business is becoming a fast emerging trend. Every five in eight companies are operating online, conducting e-commerce business. But being functional online doesn't mean you can escape legal matters.

There are various legal issues associated with e-commerce businesses as well. And if these issues are not taken care of in time, they can lead to serious problems for your business.[46]

Described below are some of the common legal issues an e-commerce business faces.

- **JURISDICTIONAL ISSUES**

The boom in internet transactions has brought a host of issues regarding jurisdiction of such transactions to the forefront. The primary question that needs to be addressed is "when a transaction takes place online, where is the contract concluded?" Justice S. Muralidhar has stated that the traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case brought before it.[47] With the internet, the question of 'territorial' jurisdiction gets complicated largely on account of the fact that the internet is borderless & Ecommerce exists in a borderless environment. Hence, create concern –

- Whose jurisdiction?
- Where to take action?
- What test and laws to be followed?
- When an individual resides outside the jurisdictional area?
- Laws of which country applies on a particular e-Commerce transaction?
- Courts/Authorities of which country are to be approached for enforcement of rights?

At present, although e-transactions are at the helm, we must realize that the laws governing these transactions are yet to emerge and develop. Although we have the IT Act in place, it is not sufficient to deal with online transactions in India. It is a step in the right direction as it lays down admissibility of electronic records, penalties for cyber-crimes etc. However, in the case of online transactions, it can be regarded as an enabling statute which must be read in consonance with the Contract Act, 1872 in order to determine whether the online transaction does indeed constitute a valid contract. There is a dire need for specific legislation to be enacted to determine

[46]Common Legal Issues Faced By E-Commerce Businesses
<https://www.eurologo.org/common-legal-issues-faced-by-e-commerce-businesses/>
[47]Jurisdictional Challenges in Online Transactions
<http://www.legalservicesindia.com/article/2268/Jurisdictional-Challenges-in-Online-Transactions.html>

issues involving jurisdiction for e-commerce disputes.

- **E-CONTRACTS**

Electronic contracts are governed by the basic principles provided in the Indian Contract Act, 1872 ("ICA"), which mandates that a valid contract should have been entered with free consent and for a lawful consideration between two adults. Section 10A of the Information Technology Act, 2000 ("IT Act") provides validity to e-contracts. So, both the ICA and IT Act needs to be read in conjunction to understand and provide legal validity to e-contracts. Further, section 3 of the Evidence Act provides that the evidence may be in electronic form. The Supreme Court in Trimex International FZE Ltd. Dubai v. Vedanta Aluminum Ltd.1has held that e-mails exchanges between parties regarding mutual obligations constitute a contract. In an online environment, the possibility of minors entering into contracts increases, more so with the increasing usage of the online medium among teenagers (read minors here) and their preference to shop online or purchase online goods/services.[48] It becomes crucial for an online business portal to keep such possibility in consideration and qualify its website or form stating that the individual with whom it is trading or entering into the contract is a major. Stamping of contracts is yet another issue.[49] An instrument that is not appropriately stamped may not be admissible as evidence unless the necessary stamp duty along with the penalty has been paid. But the payment of stamp duty is applicable in case of physical documents and is not feasible in cases of e-contracts. However, as the payment of stamp duty has gone online and e-stamp papers are available, it can become a possibility later that stamp duty might be asked on e-contracts as well.

- **DATA PROTECTION**

Security of the information provided during the online transaction is a major concern. Under section 43A of the IT Act the "Reasonable practices and procedures and sensitive personal data or information Rules, 2011" have been proposed, which provide a framework for the protection of data in India. Data can be personal, which has been defined as "any information that relates to

[48]Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management

[49] Praveen Kumar Mall, 'Emerging Trends Of E-Consumers & Determining Jurisdictional Disputes In India', International Journal Of Legal Insight, ISSN: 2456-3595, Volume I, Issue 1

a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." The date can also be sensitive and a sensitive personal data consists of password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information. The entity collecting data should have a privacy policy in place, should always obtain consent from the provider of sensitive information and maintain reasonable security practices and procedures. Unauthorized access to personal information and any misuse of such personal information should be checked by the online goods/service providers.

- **IPR (INTELLECTUAL PROPERTY RIGHTS) ISSUES**

There are enormous possibilities of trademark, copyright or patent infringements in the online medium. E-commerce websites are designed and made by other parties and often the content is also created by third parties. Unless the agreements between the parties specifically provide the IP rights, there can be serious ownership issues of IPR. Any usage of third party IPR should have valid approvals in place. In interactive websites, the disclaimer and IPR policy should clearly spell out these issues and goods/service providers should also keep a watchful eye on the usage of their websites regularly. Domain names have trademark protection and deceptively similar domain names can give rise to disputes. In Satyam Infoway Ltd v. Sifynet Solutions Pvt Ltd., the Supreme Court had held that "a domain name may pertain to the provision of services within the meaning of section 2(z) of the Trade Marks Act."

- **TAXATION ISSUES**

E-Commerce occurs in various forms and between various entities in the market. The question is how to tax it. As the Internet has crossed borders (sovereignty) how can the requirements of physical presence and substantial nexus criteria of taxation be met. Due to the uniqueness of e-commerce, taxation faces a number of problems. This articles tries to find out the key issues in the area of e-commerce taxation and tries to analyse the existing regime with regard to e-commerce taxation. It is also alarmed that if this is left untaxed, it will give rise to a parallel economy.

Difficulties in taxing e-commerce transactions:

- Determination of economic activity (to avoid double taxation)
- Identification of the existence of permanent establishment
- Tracing commencing and endpoint of transaction
- Lack of documentation to know the nature of the contract.

The Indirect tax laws need to be evolved and redesigned to consider the changing business dynamics of e-Commerce since the activities involve high volume and low-value supplies.

- **PRIVACY AND SECURITY**

Data protection is becoming an increasingly important issue for customers in e-commerce. Collection and the storage of personal data of the costumers should be made lawfully, with the implementation of adequate measures and modern technical resources for the protection of the personal data of the costumers.[50] The Law on Personal Data Protection requires the trader to be registered as a data administrator into the register of the Personal Data Protection Commission. The law describes in details the obligations of the administrators of personal data. E-commerce websites must have a policy for personal data protection that is available and posted in a conspicuous place on the site. Published rules for the protection of personal data must be drafted in compliance with the law.

- **RETURN POLICY**

The Law on consumer protection which regulates the sales in e-commerce contains an unambiguous provision for the right of every customer to return the purchased goods within seven days term after the delivery. The law does not require the presence of defects or inconsistency in the good quality; neither any reason for return has to be mentioned. The conditions upon which the right of return of goods purchased over the Internet cannot be exercised by the user are explicitly listed in the law. In any other case, the entrepreneur should respect the legal right of the customer and should accept back the purchased goods upon the existence of the conditions for returning.

[50] Dr Harish Kumari, 'Commerce In India-Challenges And Legal Issues', International Journal Of Business 29 Management, Vol 2(1), 2015 Available at <www.ijbm.co.in>

The legal framework for e-commerce is increasingly becoming complex even in one single jurisdiction. Things become more and more complicated when you are faced simultaneously with hundreds of potentially applicable legislation because you are entering agreements with customers located anywhere in the world.

The Internet provides many new sales and marketing opportunities and online business must adapt to this changing commercial environment.

- **ADVERTISING**

Advertising is an important and legitimate means for a seller to awaken interest in his products. For long, advertisements were regulated by the courts, government, tribunals, or police that depended upon the nature of each case. Additionally, the absence of single comprehensive legislation created a lot of confusion in terms of proper code to follow by the industry and the authority to regulate or guide the pattern of advertising. In 1985, the Advertising Standards Council of India ("ASCI"), a non-statutory tribunal, was established that created a self-regulatory mechanism of ensuring ethical advertising practices. ASCI entertained and disposed off complaints based on its Code of Advertising Practice ("ASCI Code"). On certain occasions, however, the ASCI orders were set aside by courts as ASCI being a voluntary association was considered usurping the jurisdiction of courts when it passed orders against non-members. Gradually, the ASCI Code received huge recognition from the advertising industry. The warnings issued by ASCI to the advertisers against the misleading advertisements were gradually being accepted by the advertisers and the advertisements were actually stopped being aired or were modified significantly to comply with the prescribed ASCI Code. The advertisements should make truthful and honest representations and avoid false and misleading claims, should not be offensive to public decency or morality, not promote products which are hazardous or harmful to society or to individuals, particularly minors, observe fairness in competition keeping in mind consumer's interests and avoid obscene or harmful publication and indecent representation of women.

- **COMPETITION**

E-commerce has already generated a lot of competition with ever-increasing players and acquisition of several old players in the market and has enabled the development of new services, new distribution channels, and greater efficiency in business activities. Creation e-hubs where significant market share lies can lead to certain competition issues if they appear to have developed sustainable market power resulting from network effects and/or engaging in strategic acts to preserve or maintain their market power. Potential issues for e-commerce players would be price-fixing or tacit collusion or anti-competitive discrimination or refusal of access to third parties. E-commerce players should refrain from collusion and excessive pricing. Options for parties to use the same web platform for different kinds of products/services can give rise to different intermediaries and that can lead to collusive behaviour. Market transparency should be encouraged.

1.3 SECURITY CHALLENGES OF E-COMMERCE

Security risks associated with e-commerce can be as a result of human error, an accident or unauthorized access to systems. E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error.[51]There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are phishing attacks, money thefts, data misuse, hacking, credit card frauds, and unprotected services.[52]

- **CREDIT CARD FRAUD**

Credit card fraud is the most common security threat that online retailers face. It occurs when a hacker gains unauthorized access to customers' personal and payment information. To access this data, the hacker may penetrate the database of an e-commerce site using malicious software

[51] Aziz, Dhiyauddin&Zunawanis, &Shahrulnizam, (2016) E-Commerce Challenges and Solutions
[52]What is e-commerce and what are the major threats
<https://www.techgenyz.com/2017/04/05/e-commerce-major-threats-e-commerce-security/>

programs. At times, a hacker's intention when stealing customers' data is to sell it on black markets.[53]

- **DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS**

This type of security threat aims at taking down an online retail store by sending overwhelming requests to its servers. The attacks originate from thousands of untraceable IP addresses. When this type of threat hits the servers, they slow down or completely shut down. An e-commerce site can also go offline temporarily when a DDoS attack affects its servers.

- **MAN-IN-THE-MIDDLE ATTACKS**

As hackers are becoming smarter with technology, they are devising ways of listening to the communications made by users of an e-commerce website. Through an approach known as a man-in-the-middle attack, these hackers maliciously trick users into connecting to a public wireless network. They gain access to people's devices once they are on public wireless networks. Hackers get to see a people's browsing history, credit card numbers, passwords and usernames if the websites they are visiting lack strong encryptions.

- **BOTS**

Bots, either good or bad, are all over the worldwide web. Search engines such as Bing and Google use good bots for indexing search results. On the other hand, there are hackers that use malicious bots for gathering data such as product data, inventories and pricing data. These bots are also capable of accessing the database of an e-commerce site and listing the logins of user accounts.[54]

- **MALWARE**

In information technology, malware simply refers to malicious software programs. Attackers usually inject web pages or files with these malicious programs to help them in gaining access to

[53]Patro, Sibo&Padhy, Neelamadhab&Panigrahi, Rasmita.(2016) Security Issues over E-Commerce and their Solutions IJARCCE. 5. 81-85. 10.17148/IJARCCE.2016.51216

[54] A Sengupta, C Mazumdar "e-commerce security – a life cycle approach" sadhanavol 30, parts 2 & 3, April/June 2005

online retails stores. Through means such as SQL injection, they can easily insert the malware into a website's database allowing it to compromise the data stored in the database.

- **PHISHING SCAMS**

E-commerce sites are also prone to phishing scams sent by known or unknown people in the form of emails. These scams focus on targeting important user data like credit card numbers and login credentials. An attacker may use a scheme known as social engineering to lure online shoppers to give out their personal information. When sent in an email to an online shopper, a phishing scam may contain a link to a malicious site that resembles an e-commerce site.

- **PRICE MANIPULATION**

Modern e-commerce systems often face price manipulation problems. These systems are fully automated; right from the first visit to the final payment getaway. Stealing is the most common intention of price manipulation. It allows an intruder to slide or install a lower price into the URL and get away with all the data.

- **SNOWSHOE SPAM**

Now spam is something which is very common. Almost each one of us deals with spam emails in our mailbox. The spam messages problem has never been actually solved, but now it is turning out to be a not so general issue. The reason for this is the very nature of a spam message. Spam is something which is sent by one person, but unfortunately, new development is taking place in the cyber world. It is called as snowshoe spam. Unlike regular spam it is not sent from one computer but is sent from many users. In such a case it becomes difficult for the anti-spam software to protect the spam messages.

1.4 BEST PRACTICES TO COMBAT E-COMMERCE SECURITY THREATS

- **PCI DSS COMPLIANCE**

PCI DSS stands for Payment Card Industry – Data Security Standard.

PCI standard contains a series of security requirements that every business, big or small, must

follow.[55] It is designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The PCI DSS compliance mandates creating and maintaining a security policy that covers different security aspects, such as installing firewalls and data protection mechanism. Businesses have to encrypt cardholder data that is transmitted over public networks; they need to establish strong passwords and monitor access to account data. PCI DSS can immensely help e-commerce companies to build their internal information security program, and design it to meet their own business needs.

- **USE SSL CERTIFICATES**

SSL (Secure Sockets Layer) certificates can be the crucial cybersecurity measures for your online store in order to protect your business data as well as your customers' information from attack. Adding an SSL certificate puts a lock icon and https to the web address that creates an encrypted link and prevents an attacker from listening in to the traffic. When an encrypted SSL link is created, what happens immediately is a user's web browser verifies that the site on the other end is who it says it is.[56] If you ignore this step, it may lead to a MITM attack. There are different SSL certificate versions: domain validation, organization validation, and extended validation.

- **ADDRESS VERIFICATION SYSTEM (AVS)**

An AVS is a system that validates a customer's entered address by comparing with major shipping carriers. This verification process can effectively reduce the number of checkout errors, and increase the conversion rate in the process. AVS can be both domestic and international, and you should be ready to handle both AVSs' result codes. It would be important to know how AVS can be helpful. Suppose an individual steals one of your customers' credit card information, then he may have obtained customer's name, credit card number, and possibly CVV code. But the thief doesn't know the address linked to that particular credit card account. Only the true cardholder would have that information. So, you and your customers are better protected when

[55]Alexander Menzheres, 'Recent E-Commerce Security Issues And Best Practices (2018)' (*Eteam.io*, 2020) <https://www.eteam.io/blog/e-commerce-security-issues>
[56](*Csie.ntu.edu.tw*, 2020) <https://www.csie.ntu.edu.tw/~ec/Laudon/Chapter5.pdf>

fraud disputes arise.

- **WEB APPLICATION FIREWALLS (WAF)**

Usually, network firewalls are unable to block the port through which HTTP traffic is served to the web, which is why web-based application attacks have been mounting in the past few years. So web application firewalls can solve this problem by analyzing applying rules to HTTP traffic. Gartner reported that 75% of all web attacks occur at the Application Layer (Layer 7) of the Open Systems Interconnection model. WAFs are specifically designed to protect both inbound and outbound web traffic directed to a particular web server. WAFs are highly beneficial for an e-commerce business as they rely on private user data on their websites. WAFs automatically filter out malicious web traffic and allow you to manually dictate who you want to access to your website.[57]

- **BOT BLOCKERS**

Bot blockers are basically software programs that monitor the traffic coming to your website and find patterns that tell you if a bad bot is harvesting your site's content. When a blocker detects a bot, it usually drops the request, and as a result, the robot discontinues making data requests. These blocking adjustments often happen in real-time. Some bot blockers are sophisticated and evaluate the specific request patterns, HTTP headers, source address, page request behaviours and more. For example, CAPTCHA is the first layer of defence that tests threatening visitor quickly and weed out automated bots, which cannot read and supply a correct answer to the test.

1.5 ISSUES AND CONCERNS IN NEWLY DRAFTED E-COMMERCE POLICY BILL OF INDIA

Single legislation to address all aspects of e-commerce would be enacted and a single regulator would be set up to consider issues such as:[58]

- Addressing the legal fragmentation seen across the various laws governing the

[57] Tan and Thoen (2000), <http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/1812>
[58]Electronic Commerce in India: Draft National Policy Framework
<https://www.readkong.com/page/electronic-commerce-in-india-draft-national-policy-9057835>

e-commerce sector, viz. the Information Technology Act, 2000, the consumer protection laws, and other relevant legislation/ rules and ensuring uniformity in the definition of the various e-commerce players and levels of the obligation imposed on them.

- FDI implementation issues
- Consumer protection issues
- Central registry/ repository dealing with promoting domestic production, full disclosure by e-commerce entities of purpose and intent etc.
- Reporting and information requirements
- Setting up an accreditation system for vetting e-commerce platforms which adhere to good business practices.

The data localization is one of the contentious issues in the draft bill which was resolved by commerce ministry and decided to keep data localization norms out of the final policy, leaving the proposed data protection legislation to deal with the matter.

1.6 FUTURE OF E-COMMERCE

In spite of a few challenges, still, e-commerce is booming day by day and sooner will become the drastic demand of the users.[59] The future of e-commerce is bright and growth will come from mobile platforms, personalization, social media analytics, omnichannel service, and sharing economy business models.[60]

Following are some future trends of e-commerce:

- **SOCIAL MEDIA**

Majority of online buying decisions are made on Social Media. A social network like Facebook, LinkedIn, Twitter, Google+, Pinterestetc have become a medium for easy log-in and purchase. Moreover, the clients can stay updated via the posts published on this media. Further, the

[59] Choi, Soon-Yong &Whinston, Andrew (1999)The Future of E-Commerce: Integrate and Customize Computer 32. 133 - 134, 138. 10.1109/2.738310.
[60]Future of E-Commerce Business In India - HunterTech Global <http://huntertechglobal.com/2019/04/16/future-scope-e-commerce-business-india/>

advertising & promotions on these social sites have increased the chances of success of generating transactions to many folds.[61]

- **DRONE DELIVERY**

Companies have been working their way around to innovate the delivery process to shorten human effort as well as time. The answer to these problems is Delivery by Drones. DGCA is now fast-tracking the process of issuing guidelines for the use of drones for civil purposes in India. If everything goes as per the plan, then India might become the first country in the world to allow the use of drones for civil purposes.[62]

- **APP ONLY APPROACH**

Statistics suggest the future of the internet lies in mobiles. Experts say more than 580 million people in India will use the Internet by 2018, and 70-80% of them will access the Web on mobile phones. This will cause all major players to switch to app-only model. About two-thirds of its online traffic of Flipkart comes from users in small cities and towns.[63]Flipkart's app-only approach assumes larger significance in these places where most people don't own desktop computers and have limited access to broadband.

- **GOOGLE'S BUY NOW BUTTON**

Google is reportedly working on its own "Buy Now" style button that would allow e-shoppers to search for products on Google and purchase them with a single click, right through Google's own search results page. The button will be displayed near sponsored search results beneath a "Shop on Google" heading at the top of the page. When users click on the Google's "Buy Now" button, they will be re-directed to another Google page that will allow them to choose specific item details, such as colour and size, and then select a shipping route. Google would then pass on the order information, including the customer's name and shipping address, to the retailer.[64]

- **ARTIFICIAL INTELLIGENCE**

[61]Challenges and Future Scope of E-commerce in India <https://www.ijettcs.org/Volume5Issue2/IJETTCS-2016-04-23-93.pdf>
[62]STUDY OF FUTURE SCOPE AND CHALLENGES OF ONLINE RETAIL <https://arseam.com/sites/default/files/published-papers/p1i9v5ijmfm-Full-%2001-09%20MANOJ%20SHARMA%20-PRAMOD%20GUPTA%20Sep-2017_0.pdf>
[63]Supra note 12
[64](*Criteo.com*, 2020) <https://www.criteo.com/es/wp-content/uploads/sites/8/2017/09/ovum-the-future-of-e-commerce-the-road-to-2026.pdf>

As the e-commerce space gets saturated, investors looking for innovative use of technology are zeroing in on companies developing artificial intelligence (AI) solutions. Jet Airways is experimenting with one such solution devised by Vizury.

1.7 LET'S SUM UP

In this chapter, we have studied how E-commerce can bring immense benefit both to the buyers and the sellers.But it has not developed to the level as was envisaged. It is because it is not freefrom problems. These are, security problem, the poor spread of Internet facility, lackof face-to-face contact, taxation problem, the problem of intellectual property rightviolation etc. Some of these problems have been addressed by the enactment of laws.We are confident that all the problems will be addressed in the course of time and itwill become the most popular mode of commerce.E-commerce has immense potential to generate wealth for developing countries. Enacting legislation in order to facilitate E-commerce transactions is merely the first step. Effective implementation and strategic exploitation of its potential is a much more arduous task and should be done with care and caution.

1.8 FURTHER READING

- Sumanjeet (2011), 'Emerging Economic Models in the Age of Internet and E-commerce,' Global Journal of Business Management and Information Technology, Vol. 1, No.1, Pp. 53–68.
- Bulsara, Hemantkumar&Vaghela, Pratiksinh. (2017). E-COMMERCE: PAST, PRESENT AND FUTURE - AN INDIAN PERSPECTIVE.
- Dasgupta, Prithviraj. &Sengupta, Kasturi. (2002). E-Commerce in Indian Insurance Industry. Electronic Commerce Research, Vol. 2, 43-60.
- Raghunath, Alka. &Panga, Murlidhar. (2013). Problem and Prospects of E-Commerce. International Journal of Research and Development- A Management Review, Vol. 2, 59-66

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the jurisdictional issues involved in e-commerce?**

- Whose jurisdiction?
- Where to take action?
- What test and laws to be followed?
- When an individual resides outside the jurisdictional area?
- Laws of which country applies on a particular e-Commerce transaction?
- Courts/Authorities of which country are to be approached for enforcement of rights?

2. **What are the issues in the newly drafted e-commerce policy bill?**

- Addressing the legal fragmentation seen across the various laws governing the e-commerce sector, viz. the Information Technology Act, 2000, the consumer protection laws, and other relevant legislation/ rules and ensuring uniformity in the definition of the various e-commerce players and levels of obligation imposed on them.
- FDI implementation issues
- Consumer protection issues
- Central registry/ repository dealing with promoting domestic production, full disclosure by e-commerce entities of purpose and intent etc.
- Reporting and information requirements
- Setting up an accreditation system for vetting e-commerce platforms which adhere to good business practices.

3. **Write a few security challenges of e-commerce?**

- Credit card fraud
- Distributed denial of service (DDoS) attacks
- Man-in-the-middle attacks
- Bots
- Malware

1.10 ACTIVITY

Elucidate the legal and security challenges faced in E-commerce along with suggestions pertaining to it? Explain it with relevant cases? (1000 – 1500 words)

Unit 4: Taxing E-Commerce 4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Changing face of Brick n' Mortar Model

1.4 Uniqueness of E-commerce

1.5 The basis of taxation in Online Environment

1.6 Constituting permanent establishment

1.7 OECD Model Treaty: A Critique

1.8 OECD Model Treaty and E-commerce

1.9 Changes to the commentary on Article 5

1.10 Whether a Website Acts as a PE?

1.11 Whether a Server Acts as a PE?

1.12 An ISP hosting a website

1.13 An enterprise hosting its own website

1.14 Let's sum up

1.15 Further reading

1.16 Check your progress: Possible answers

1.17 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The basis of taxation in online environment
- OECD Model Treaty and E-commerce
- Changes to the commentary on Article 5

1.2 INTRODUCTION

E-commerce is a new wat of conducting, managing and executing business transactions using information technology tools. E-commerce is commerce based on bytes.[65] The World Trade Organization (WTO) Ministerial Declaration on E-commerce defines "e-commerce" as "the production, distribution, marketing, sales or delivery of goods and services by electronic means."[66] And according to the Internet Tax Freedom Act "e-commerce," includes "any transaction conducted over the Internet or through Internet access, comprising the sale, lease, license, offer, or delivery of property, goods, services, or information, whether or not for consideration, and includes the provision of Internet access."[67]

1.3 CHANGING FACE OF BRICK N' MORTAR MODEL

E-commerce has changed the 'brick and mortar' world of physical commerce to 'click and mortar', 'click and brick' and 'all clicks' online commerce. These online commerce models have characteristics of their own.[68]

Brick n' Mortar	**Click n' Mortar**	**Click n' Brick**	**All Clicks**
Purely offline (physical).	Partly offline and partly online.	Partly offline and partly online.	Purely online.
No web presence.	Web presence supplements offline activities.	Web presence complements the offline activities.	No offline presence.
Marketing and selling goods in an offline environment only.	Marketing and selling goods in both offline and online environment.	Increasingly shifting marketing and selling activities to the online environment.	Marketing and selling of Information (Knowledge or content) only.

[65]Defining e-commerce <https://cn10xz.blogspot.com/2012/10/defining-e-commerce.html>

[66]The six main instruments of e-commerce that have been recognized by WTO are telephone, fax, TV, electronic payment and money transfer systems, EDI and Internet

[67]47 U.S. Code § 151 - Purposes of chapter; <https://www.law.cornell.edu/uscode/text/47/151>

[68]Jones, Richard &Basu, Subhajit. (2002) Taxation of Electronic Commerce: A Developing Problem. INTERNATIONAL REVIEW OF LAW COMPUTERS &TECHNOLOGY 16. 35-52. 10.1080/13600860220136093

Handle tangible goods.	Handle tangible goods.	Handle tangible goods.	Handle intangible goods.

The Government has always been taxing brick n' mortar businesses as per the statutory provisions. It establishes the boundaries of legitimate state authority to impose a duty to collect sales and use taxes and reduces litigation concerning those taxes. So far, the brick n' mortar businesses are being taxed on the principles of physical presence or 'substantial nexus' criteria.

The "click and mortar" sellers are required to collect sales taxes based on their substantial nexus in a state where their product is delivered. Presumably, the point of sale is the state to which the goods are shipped, and thus, the consumer owes sales taxes to this state. These are like mail-order companies, delivering tangible products via a common carrier.[69]

It is important that transactions should not be immune from taxation solely because the sale is conducted through a medium distinct from that of a traditional brick-and-mortar retailer. Similarly, it is not prudent to tax these e-commerce models purely on the basis of the traditional approach to 'brick n' mortar' taxation as they have their unique features.

1.4 UNIQUENESS OF E-COMMERCE

Tax revenues are a major source of income to the Governments. One major concern is whether a shift to online commerce may have a major impact on whether such a transaction will result in tax revenues, and if so, which taxing authority has the right to those revenues. It is the nature of the 'technology-based transactions' which has given rise to:

a) The lack of 'physical' connection between a consumer in one state and a seller in another state;
b) Ever-changing location of web servers hosting the website, meant for online transactions;
c) Relocation of businesses in tax havens;

[69] DJ Johnston, Secretary-General of the OECD 'Taxation and social progress' Editorial The OECD Observer No 215, January 1999, <www.oecd.org/publications/observer/215/e.toc.htm>

d) General confusion regarding which country has the right to tax the transaction, and at what rate;
e) Non-taxation of digital (intangible) goods, like software, music and data (or information);
f) Export and import of digital (intangible) goods across international borders without paying customs duty (or tariffs), thereby bypassing the existing export-import policies, regulations and tax systems;
g) A parallel channel of transactions, ignoring the traditional documents based banking practices;
h) The general lowering down of 'barriers to trade' for the smaller business entities; and
i) Complete disregard to accounting and audit procedures.

Hence, any taxation regime for e-commerce has to address the aforesaid points from (a) to (i). In other words, a new tax system (or structure) is required to redefine the basis of taxation in online environment? What constitutes a 'permanent establishment'? What should be the modus operandi of collecting taxes?

It should not be forgotten that it is the nation state's constitutional prerogative to levy taxes on any online economic activity and for that purpose every nation state has a right to define its own e-commerce taxation principles. Moreover, it is a myth that electronic tax is an 'additional' tax burden – the fact is that it is a new tax which is applicable in lieu of other indirect taxes.[70]

1.5 THE BASIS OF TAXATION IN ONLINE ENVIRONMENT

The presumption is that no one wants to pay taxes. Given a chance or opportunity, every taxpayer would at least try to pay minimum of taxes. Hence, the thumb rule for wider acceptance of any new tax system is that it should not discriminate among types of commerce, nor should it create incentives that will change the nature or locations of transactions, i.e., it should observe strict neutrality. That is to say that of by going online, a vendor saves on tax, then such a tax regime would be beneficial for the vendor but detrimental for the state.

As the Organization for Economic Co-operation and Development (OECD), a 30 member organization (Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico,

[70]Indirect tax, wherein tax is levied on transactions like, Sales tax, Custom duty, Excise duty and VAT

Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States) has proposed that the basis of any online taxation system should be equitable, simple, certain, effective, distortions free, flexible and dynamic. The idea is to create a uniform mode of taxation whether offline or online. That is, any online taxation system should completely harmonize with existing offline taxation system. Broadly speaking, electronic commerce should be taxed neither more nor less heavily than other commerce, and online sales should, to the extent possible, be taxed at the state of destination of sales, irrespective of the fact whether the vendor (seller) has a physical presence in the state or not.

It is not easy to adopt the OECD proposed guidelines, as their exist certain inherent difficulties in adopting and extending offline taxation features to an online environment. More so, the technology has failed to provide any clear-cut solutions so far.

1.6 CONSTITUTING PERMANENT ESTABLISHMENT

In order to understand the basis of taxation in online environment, the primal question that needs to be answered is: what constitutes a 'physical presence' or substantial nexus'?

a) Is it downloading of the website and its contents at a particular location (buyer's place of residence)? Or
b) Is it the location of web server, hosting the website?

In fact, if one looks from the point of establishing "minimum contacts" and "purposeful availment", then it would be the nature and mode of transaction with the resident that establishes the physical presence of the seller in the forum state. It would render the seller taxable in every possible taxable jurisdiction. But if one treats presence of a web server as permanent establishment for the purpose of electronic taxation then it would be make seller solely taxable at the jurisdiction, where the server is located.

Thus it is important to understand the principle of permanent establishment as being adopted by the OECD as Model Tax Convention on Income and Capital (OECD Model Treaty).

1.7 OECD MODEL TREATY: A CRITIQUE

The OECD Model Treaty defines "permanent establishment" as a fixed place of business through which the business of an enterprise is wholly or partly carried on (Article 5(1)).[71] It defines certain types of activities, per se permanent establishments, including offices, factories, and mines. (Article 5(2)). Other types of activities are specified as not constituting a permanent establishment; for present purposes, the most important of these is the maintenance of a fixed place of business solely for the purpose of carrying in "activity of a preparatory or auxiliary character". (Article 5(4)(e)). An enterprise's use of an independent agent to carry on business activities does not create a permanent establishment. (Article 5(6)). A permanent establishment does result, however, from use of a dependant agent, one who is acting on behalf of an enterprise and has, and habitually exercises, an authority to conclude contracts in the name of the enterprise. (Article 5(5)).

Unanswered questions arose when applying the Treaty's definition of permanent establishment to electronic commerce. Does hosting a web site on a server constitute a permanent establishment where the server is located? Is a website-hosting ISP an agent of the company whose website it hosts, so as to give rise to a permanent establishment where the ISP is located? Can computer equipment that operates automatically, without human intervention, ever constitute a permanent establishment?

1.8 OECD MODEL TREATY AND E-COMMERCE

On December 22, 2000 the Committee on Fiscal Affairs adopted the Commentary on the OECD Model Treaty concerning the issue of the application of the current definition of permanent establishment (Art.5) in the context of e-commerce.[72]

The Committee has been able to reach a consensus on the various issues concerning the application of the current definition of permanent establishment in the context of e-commerce. This consensus includes:

- That a website cannot, in itself, constitute a permanent establishment;

[71] Article 5 (Permanent establishment) - swisstaxnetwork.ch
<http://sites.google.com/site/steuernetzwerk/gesetze/swiss-dta/article-5-swiss-dta>
[72] Internet transactions and PE issues.- Free Online Library
<https://www.thefreelibrary.com/Internet+transactions+and+PE+issues.-a0102024755>

- That a website hosting arrangement typically does not result in a permanent establishment for the enterprise that carries on business through that website; and
- That an ISP will not, except in very unusual circumstances, constitute a dependant agent of another enterprise so as to constitute a permanent establishment of that enterprise.[73]

However, Spain and Portugal do not consider that physical presence is a requirement for a permanent establishment to exist in the context of e-commerce, and therefore, they also consider that, in some circumstances, an enterprise carrying on business in a State through a website could be treated as having a permanent establishment in that State.

Since mainly the entrepreneur or persons carry on the business of an enterprise, who are in a paid-employment relationship with the enterprise (personnel). This is still an accurate statement of how business operates but, again, does not rule out that a business may be at least partly carried on without personnel. The Committee concluded that human intervention is not a requirement for the existence of a permanent establishment (PE), because the Committee believes that a requirement of human intervention could mean that, outside the e-commerce environment, important and essential business functions could be performed through fixed automated equipment located permanently at a given location without a permanent establishment (PE) being found to exist, a result that would be contrary to the object and purpose of Article 5.

1.9 CHANGES TO THE COMMENTARY ON ARTICLE 5

According to the new OECD Commentary, on the "OECD Model Treaty" issued on January 28, 2003, a website is "a combination of software and electronic data" and "does not in itself constitute tangible property". Paragraphs 42.1 to 42.10 have been added immediately after paragraph 42 of the Commentary on Article 5. It further clarifies:

a) Whether a website constitutes a "place of business";
b) Whether location of a server constitutes a permanent establishment (PE):

- When an ISP hosts its website, or
- When an enterprise owns (or leases) and operates the server on which the website is stored;

[73]TAX AND COMMERCE OECD CLARIFICATION ON THE APPLICATION <http://www.oecd.org/tax/treaties/1923380.pdf>

c) Whether the location of a computer equipment constitutes a permanent establishment when functions performed through that computer equipment exceeds the preparatory or auxiliary threshold.[74]

1.10 WHETHER A WEBSITE ACTS AS A PE?

An Internet website, which is a combination of software and electronic data, does not in itself constitute tangible property.[75] A website, therefore does not have a location that can constitute a "place of business" as there is no "facility such as premises, or in certain instances, machinery or equipment" as far as the software and data constituting that website is concerned.[76]

1.11 WHETHER A SERVER ACTS AS A PE?

The distinction between a website and the server on which the website is stored and used is important since the enterprise that operates the server may be different from the enterprise that carries on business through the website. In order to constitute a fixed place of business, a server will need to be located at a certain place for a sufficient period of time so as to become fixed.

1.12 AN ISP HOSTING A WEBSITE

For example, it is common for the website through which an enterprise carries on its business to be hosted on the server of an Internet Service Provider (ISP). Although the fees paid to the ISP under such arrangements may be based on the amount of disk space used to store the software and data required by the website, these contracts typically do not result in the server and its location being at the disposal of the enterprise, even if the enterprise has been able to determine that its website should be hosted on a particular server at a particular location. In such a case, the enterprise does not even have a physical presence at that location since the website is not

[74]Basu, Subhajit (2001)Taxation of Electronic Commerce Journal of Information, Law and Technology 1
[75]Does your website construes as permanent establishment <https://taxmantra.com/does-your-website-construes-as-permanent-establishment-and-taxed-accordingly-2/>
[76]Simkin, Mark & Bartlett, Graham & Shim, Jung (2011) Pros And Cons Of E-Commerce Taxation. International Business & Economics Research Journal (IBER).1. 10.19030/iber.v1i2.3894

tangible.[77] In these cases, the enterprise cannot be considered to have acquired a place of business by virtue of that hosting arrangement.

1.13 AN ENTERPRISE HOSTING ITS OWN WEBSITE

However, if the enterprise carrying on business through a website has the server at its own disposal, for example, it owns (or leases) and operates the server on which the website is stored and used, the place where that server is located could constitute a permanent establishment of the enterprise if the other requirements of the Article are met.

Such location may thus constitute a "fixed place of business" of the enterprise that operates that server.[78]

Another issue is whether the business of an enterprise may be said to be wholly or partly carried on at a location where the enterprise has equipment such as a server at its disposal. The question of whether the business of an enterprise is wholly or partly carried on through such equipment needs to be examined on a case-by-case basis, having regard to whether it can be said that, because of such equipment, the enterprise has facilities at its disposal where business functions of the enterprise are performed.[79]

Significantly, the commentary further provides where an enterprise operates computer equipment at a particular location; a permanent establishment may exist even though no personnel of that enterprise is required at that location for the operation of the equipment. The presence of personnel is not necessary to consider that an enterprise wholly or partly carries on its business at a location when no personnel are in fact required to carry on business activities at that location.

1.14 LET'S SUM UP

In this chapter, we have studied the uniqueness of e-commerce along with the basis of taxation in the online environment. We also discussed the OECD Model Treaty and its critique along with

[77]India's reservations on 2017 update to the OECD Model Tax <http://www.in.kpmg.com/taxflashnews/KPMG-Flash-News-Indias-reservations-update-to-the-OECD-Model-Tax-Convention-and-Commentary-2.pdf>

[78]Nadeem, Shariq&Saxena, A (2018) The Challenges of Taxing E-Commerce.International Journal of Management Studies V 56. 10.18843/ijms/v5i4(4)/07

[79]TAX AND COMMERCE OECD CLARIFICATION <http://www.oecd.org/tax/treaties/1923380.pdf>

the changes that need to put forth on Article 5. Finally, we ended the discussion with whether a website and server act as a PE along with an example of an enterprise hosting its website.

1.15 FURTHER READING

- Jones, Richard &Basu, Subhajit. (2002). Taxation of Electronic Commerce: A Developing Problem. INTERNATIONAL REVIEW OF LAW COMPUTERS & TECHNOLOGY. 16. 35-52. 10.1080/13600860220136093.
- Azam, Rifat. (2007). E-Commerce Taxation and Cyberspace Law: The Integrative Adaptation Model.
- Basu, Subhajit (2007), Global Perspectives of E-Commerce Taxation Law, Ashgate.
- Shepherd, Jordan (2014), "A Successful Conclusion to the WTO Bali Ministerial," King & Spalding: Trade and Manufacturing Alert.

1.16 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is Brick n' mortar model?

The Government has always been taxing brick n' mortar businesses as per the statutory provisions. It establishes the boundaries of legitimate state authority to impose a duty to collect sales and use taxes and reduces litigation concerning those taxes. So far, the brick n' mortar businesses are being taxed on the principles of physical presence or 'substantial nexus' criteria.

2) What is Click n' Mortar model?

The "click and mortar" sellers are required to collect sales taxes based on their substantial nexus in a state where their product is delivered. Presumably, the point of sale is the state to which the goods are shipped, and thus, the consumer owes sales taxes to this state. These are like mail-order companies, delivering tangible products via a common carrier.

3) What is a permanent establishment?

The OECD Model Treaty defines “permanent establishment” as a fixed place of business through which the business of an enterprise is wholly or partly carried on. It defines certain types of activities, per se permanent establishments, including offices, factories, and mines.

4) What is the main objective of the OECD Model Treaty?

The idea is to create a uniform mode of taxation whether offline or online. That is, any online taxation system should completely harmonize with the existing offline taxation system. Broadly speaking, electronic commerce should be taxed neither more nor less heavily than other commerce, and online sales should, to the extent possible, be taxed at the state of destination of sales, irrespective of the fact whether the vendor (seller) has a physical presence in the state or not.

1.17 ACTIVITY

Explain the changes that were brought into the brick n’ mortar model and how it is different from other models along with the basis of taxation? Describe the OECD Model Treaty and its advantages and disadvantages. (1000 words)

Block 2

E-Governance

Unit 1: Historical Development and Concept of E-Governance

1

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Concept of E-Governance
1.4 Historical Development of E-Governance
1.5 Good Governance versus E-Governance
1.6 Salient features of E-Governance
1.7 Objectives of E-Governance
1.8 Types of E-Governance
1.9 Let's sum up
1.10 Further reading
1.11 Check your progress: Possible answers
1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- Concept of e-governance
- Salient features of e-governance
- Different types of e-governance

1.2 INTRODUCTION

Today, citizens are becoming more and more conscious about their rights to get the required services at their doorstep and both the state and central governments recognize the need to deliver faster and efficient services to ordinary citizens through e-governance which is an

effective instrument of administration.[80] India's experience in e-governance and ICT initiatives has demonstrated significant success in improving accessibility, cutting down costs, reducing corruption and extending help and increased access to un-served groups. E-governance initiatives have reached millions of people belonging to these sections of society. It helps to improve access to information and services because these have provided economic and social development opportunities, facilitated participation and communication in policy and decision-making processes and empowered the weakest groups. This has led to the fostering of a sense of ownership and the building of social capital, which in turn, constitutes a basis for local revitalization.[81]

1.3 CONCEPT OF E-GOVERNANCE

The use of Information Technology aids to improve the ability of government to address the needs of society. It includes the publishing of policy and programme related information to transact with citizens. It extends beyond the provision of on-line services and covers the use of IT for strategic planning and reaching development goals of the government.E-governance may be defined as delivery of government services and information to the public using electronic means. Such means of delivering information is often referred to as Information Technology or 'IT' in short forms. Use of IT in government facilities is an efficient, speedy and transparent process for disseminating information to the public and other agencies, and for performing government administration activities. The term governance may be described as the process by which society steers itself. In this process, the interactions among the State, Private Enterprise and Civil Society are being increasingly conditioned and modified through the influence of Information and Communication Technologies (ICTs), constituting the phenomenon of e-Governance. Examples of these shifts in dynamics are exemplified by:[82]

i. The use of the Internet by Civil Society, NGO's and professional associations

[80]Challenges of Implementation of E-Governance <https://rrjournals.com/wp-content/uploads/2020/01/1132-1135_RRIJM190401242.pdf>
[81]A PROJECT ON E-GOVERNANCE- rotiodisha.nic.in <http://rotiodisha.nic.in/files/29102018/Publication%20And%20Training%20Material/Project%20Reports%20of%20Trainees/E-Governance/GIRIJA%20SANKAR%20MALLIK_18th%20Batch.pdf>
[82]The History of E-Gov - Term Paper <https://www.termpaperwarehouse.com/essay-on/The-History-of-E-Gov/213307>

to mobilize opinion and influence decision-making process that affect them.

ii. The increasing electronic delivery of government and commercial service and Information.

iii. The electronic publication of draft legislation and statements of direction for public feedback.

iv. On the infrastructure side, the liberalization of telecommunication markets and trends towards web-enabled mobile telephony and digital television are facilitating this evolution.

1.4 HISTORICAL DEVELOPMENT OF E-GOVERNANCE

Recognizing the increasing importance of electronics, the Government of India established the Department of Electronics in 1970. The subsequent establishment of the NIC in 1977 was the first major step towards e-governance in India as it brought 'information' and its communication to focus.[83] In the early 1980s, the use of computers was confined to very few organizations. The advent of personal computers brought the storage, retrieval and processing capacities of computers to government offices. By the late 1980s, a large number of government officers had computers but they were mostly used for 'word processing'. Gradually, with the introduction of better software, computers were put to other uses like managing databases and processing information. Advances in communications technology further improved the versatility and reach of computers, and many government departments started using ICT for a number of applications like tracking the movement of papers and files, monitoring of development programmes, processing of employees' payrolls, generation of reports etc. The main thrust for e-governance was provided by the launching of NICNET in 1987 – the national satellite-based computer network. This was followed by the launch of the District Information System programme of the National Informatics Centre (DISNIC) to computerize all district offices in the country for which free hardware and software was offered to the State Governments. The concept of e-governance has its origins in India during the seventies with a focus on the development of in-house

[83]E-Governance: A move towards paperless Administration in India <http://ijcttjournal.org/Volume4/issue-3/IJCTT-V4I3P141.pdf<

government applications in the areas of defence, economic monitoring, planning and the deployment of IT to manage data-intensive functions related to elections, census, tax administration etc.[84] The efforts of the NIC to connect all the district headquarters during the eighties was a very significant development. From the early nineties, IT technologies were supplemented by ICT technologies to extend its use for wider sectoral applications with policy emphasis on reaching out to rural areas and taking in greater inputs from NGOs and the private sector as well. There has been an increasing involvement of international donor agencies under the framework of 'e-governance for development' to catalyse the development of e-governance laws and technologies in developing countries. E-governance in India has reached the 'transactional' stage and provides various services to citizens and business and government organizations and is dispensed by central government agencies and different state government departments. ***The National e-Governance Plan (NeGP),*** initiated in 2006, attempts to make all Government services accessible to the common man in his locality, through CSCs being set up across India. The Second Administrative Reforms Commission was set up with the intention of revamping the public administration system. The eleventh report of the commission, submitted during January 2009, stresses upon to achieve a transparent, accountable and efficient governance system in the country. The commission expects the government to prepare a clear roadmap with specific milestones for transforming the citizen-government interaction at all levels to the e-governance mode by 2020.[85] This strong recommendation of the commission has led to the clearance of "Electronic Delivery of Services Bill" by the Union Cabinet during 2013 as per which the centre and state governments are required to deliver services to citizens in electronic mode. Other e-governance-related key strategic interventions for strengthening service delivery at grassroots include the constitution of Unique Identification Authority of India (UIDAI) and e-Panchayat Project of the Ministry of Panchayat Raj under Bharat Nirman II Programme. The UAIDI is mandated to provide unique identification to residents of India. The unique identification (popularly known as AADHAR) is expected to serve as the basis to ensure efficient delivery of services and act as a tool for effective monitoring of government programmes and schemes. The e-Panchayat project which aims at providing broadband

[84]IMPLEMENTING E-GOVERNANCE IN INDIA
<https://www.jstor.org/stable/42742751>
[85]E Governance, E Governance Applications, E - IAS EXAM
<https://www.civilserviceindia.com/subject/General-Studies/notes/e-governance.html>

connectivity to all village Panchayats, is expected to boost development at grassroots through bottom-up planning. As mentioned earlier, the NeGP, which was once considered a flagship government programme, has not delivered as per expectations. Most of the projects launched under NeGP are found to be lacking in terms of necessary re-engineering of underlying processes, use of emerging technologies, application of e-governance standards, localization of contents, etc. Projects initiated under NeGP are, therefore, considered to be performing at sub-optimal level. To address this E-Governance in India the government has launched e-Kranti as part of the Digital India Programme. All the ongoing and new MMPs are required to follow the key principles of e-Kranti which are: 'Transformation and not Translation', 'Integrated Services and not Individual Services', Mandatory 'Government Process Reengineering (GPR), 'ICT Infrastructure on Demand', 'Cloud by Default', 'Mobile First', 'Fast-Tracking Approvals', 'Mandating Standards and Protocols', 'Language Localization', 'National GIS (Geo-Spatial Information System)', 'Security and Electronic Data Preservation' . All the existing MMPs are to be revamped accordingly under the e-Kranti programme. With the addition of 13 more MMPs, the e-Kranti programme comprises 44 MMPs as on December 2015.

1.5 GOOD GOVERNANCE VERSUS E-GOVERNANCE

GOOD GOVERNANCE

The concept of "governance" is not new. It is as old as human civilization. Simply put "governance" means: the process of decision-making and the process by which decisions are implemented (or not implemented). Governance can be used in several contexts such as corporate governance, international governance, national governance and local governance.Good governance has 8 major characteristics. It is participatory, consensus-oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive and follows the rule of law.[86] It assures that corruption is minimized, the views of minorities are

[86]Qualities of Effective Leadership and Its impact on Good Governance <https://www.abyssinialaw.com/blog-posts/item/1473-qualities-of-effective-leadership-and-its-impact-on-good-governance>

taken into account and that the voices of the most vulnerable in society are heard in decision-making. It is also responsive to the present and future needs of society.

E-GOVERNANCE

Although the term e-Governance is widely used, there is no standard definition of this term and different governments and organizations define the term to suit own aims and objectives. Some widely used definitions are noted below:

According to World Bank, e-Governance refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve avariety of different ends, better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth and cost reductions. World Bank stress is on the use of ICT in improving citizen-government interactions, cost-cutting and transparency in the process.[87]

UNESCO defines e-Governance as ―Governance refers to the exercise of political, economic and administrative authority in the management of a country‘s affairs, including citizen‘s articulations of their interests and exercise of their legal rights and obligations. e-Governance may be understood as the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public and to other agencies while performing government administration activities.

This definition visualizes the use of ICT in the management of the country‘s affairs with greater transparency and efficiency protecting citizen‘s interests

Dr APJ Abdul Kalam, former President of India, has visualized e-Governance in the Indian context as ―A transparent smart e-Governance with seamless access, secure and authentic flow

[87]ICT and Governance | Study Notes | UGC NET Paper 1
<https://www.scholarify.in/ict-and-governance/>

of information crossing the inter-departmental barriers and providing a fair and unbiased service to the citizen.[88]

E-Governance is the application of information and communication technologies to transform the efficiency, effectiveness, transparency, and accountability of informational and transactional exchanges within government, between government and government agencies of national, state, municipal and local level, citizens and businesses and to empower citizens through access and use of information.

Electronic Governance can be defined as giving citizens the choice of when and where they access government information and services. The advantages are plenty, a higher degree of transparency, lesser paperwork, less delay, improved pace and effectiveness of governance to name a few.

1.6 SALIENT FEATURES OF E-GOVERNANCE

E-Governance is more than just a government website on the Internet. But what is it exactly, and what is it not? Many definitions exist for e-Governance. Several other terms are also commonly used, including e-business, e-democracy and e-government. E-democracy refers to the processes and structures that encompass all forms of electronic interaction between Government (elected) and the Citizen (electorate). E-government is a form of e-business in governance and refers to the processes and structures pertinent to the delivery of electronic services to the public (citizens and businesses), collaborating with business partners and conducting electronic transactions within an organizational entity. The system of e-Governance is supported by five major pillars *viz*; Computers, Connectivity, Content, Consumer/s and Confidence Building.[89]

"Computers" in this context refers to all the hardware and software requirements of Governance. "Connectivity" refers to all the information carrier systems, bandwidth etc.

[88]Information and communication technologies
<http://www.srjis.com/pages/pdfFiles/146805725525.%20TUHINA1.pdf>
[89]E-GOVERNANCE - Radome.in
<https://engg-project.blogspot.com/2010/10/e-governance.html>

"Content" refers to the information that is exchanged between the "Consumers" of the system. "Consumers" refers to all the human and human substitute systems that access and use the "Content" in the EG system.

"Confidence Building" refers to such of those measures that help the Citizens develop confidence in the e-Governance and encourages them to take to the E-Transformation. It is in this context that "Law" has a part to play along with "Education".[90]

Imagine a situation in which all interaction with government can be done through one counter 24 hours a day, 7 days a week, without waiting in lines. In the near future this will be possible if governments are willing to decentralize responsibilities and processes, and if they start to use electronic means such as the Internet. Each citizen can then contact the government through a website where all forms, legislation, news and other information will be available. In Europe and the USA, commercial banks have already adopted this approach. Most transactions can be done at an ATM, by mail or by the Internet, which has saved banks enormous costs. In other words, they do more work.

1.7 OBJECTIVES OF E-GOVERNANCE

Following are the objectives/aims of E-Governance:

1. To build an informed society – An informed society is an empowered society. Only informed people can make a Government responsible. So providing access to all to every piece of information of the Government and of public importance is one of the basic objectives of E-Governance.

2. To increase Government and Citizen Interaction - In the physical world, the Government and Citizens hardly interact. The amount of feedback from and to the citizens is very negligible. E-Governance aims to build a feedback framework, to get feedback from the people and to make the Government aware of people's problems.

[90] Singh, Rubee (2018) Impact of E-Governance in India : Opportunities & Challenges

3. To encourage citizen participation - True democracy requires the participation of each individual citizen. Increased population has led to representative democracy, which is not democracy in the true sense. E-governance aims to restore democracy to its true meaning by improving citizen participation in the Governing process, by improving the feedback, access to information and overall participation of the citizens in the decision making.

4. To bring transparency in the governing process - E-governance carries an objective to make the Governing process transparent by making all the Government data and information available to the people for access. It is to make people know the decisions and policies of the Government.

5. To make the Government accountable - Government is responsible and answerable for every act decision taken by it. E-Governance aims and will help make the Government more accountable than now by bringing transparency's and making the citizens more informed.

6. To reduce the cost of Governance - E-Governance also aims to reduce the cost of governance by cutting down on expenditure on physical delivery of information and services. It aims to do this by cutting down on stationery, which amounts to most of the government's expenditure. It also does away with the physical communication thereby reducing the time required for communication while reducing cost.

7. To reduce the reaction time of the Government – Normally due to red-tapism and other reasons, the Government takes long to reply to people's queries and problems. E-Governance aims to reduce the reaction time of the Government to the people's queries and problems, because problems are basically the Government's problems as the Government is for the people.

1.8 TYPES OF E-GOVERNANCE

E-Governance services can be shared between citizens, businessman, government and employees. These four models of e-governance areas[91]:-

1. **Government to Citizens (G2C)**
2. **Government to Government (G2G)**
3. **Government to Employees (G2E)**
4. **Government to a Businessman (G2B)**

Government to citizens (G2C):-This model of e-governance refers to the government services which are shared by citizens. Here, citizens visit the link of services that they want to use. This model strong the bond between the government and its citizen. Type of services which are provided by this model includes: -

- Payment of online bills such as electricity, water, telephone bills etc.
- Online registration of applications.
- Copies of land-record.
- Online filling of complaints.
- Availability of any kind of online information.

Government to Government (G2G):-This model refers to the services which are shared between the governments. There is lots of information that need to be shared between various government agencies, department and organizations. These types of services or information are as:-

- Sharing of information between the policedepartment of various state.
- Government document exchange which includes preparation, approval, distribution and storage of all governmental documents is also done through e-governance.
- Most of the finance and budget work are also done through e-governance.

[91] Subramanian, C (2012) E-GOVERNANCE: A KEY TO GOOD GOVERNANCE IN INDIA International Journal of Scientific Research 3 305-308

Government to businessmen (G2B):-Through this model, the bond between the private sector and government increase and businessmen use to communicate. They share information through this model like:-

- Collection of taxes.
- Rejection and approval of patent are also done by this model.
- Payment of all kind of bills and penalty.
- Sharing of all kind of information, rules and data.
- Complaints or any kind of dissatisfaction can be shown by this.

Government to employees (G2E):-This model increases the transparency between the government and its employee. Here, the employee can keep a check on the functioning and working of government and government can keep on its employees. Information that can be shared by this model:-

- All kind of data submission (attendance record, employee record etc.) from various government offices is done by this model
- An employee can file all kinds of complaints and dissatisfaction by this model.
- All kind of rule- regulation and information for employees can be shared by this.
- Employees can check their payment and working record.
- Employees can register all kind of working forms online.

1.9 LET'S SUM UP

In a nutshell, when we talk about e-Governance in India, it signifies a standard relationship between a citizen and that of the Government. In this G2C relationship, the government is liable to provide services ranging over domains like healthcare, transportation, education, telecommunications and much more. In lieu of Digital India, the country is on the surge of change and revolution. It would be evident to mention that things which are not dynamic today are considered out-fashioned.

1.10 FURTHER READING

- Grönlund, Åke& Horan, Thomas. (2004). Introducing e-Gov: History, Definitions, and Issues. Communications of the Association for Information Systems. 15. 713-729. 10.17705/1CAIS.01539.
- Brown, Mary M. 2007. Understanding E-Government Benefits: An Examination of Leading-Edge Local Governments. American Review of Public Administration 37 (2): 178 – 97.
- Chen, Yu-Che, and James Perry. 2003. Outsourcing E-Government: Managing for Success. Public Performance and Management Review 26 (4): 404 – 21.
- NandanKamath, Law Relating to Computers Internet and E Commerce Universal Law Publisher, 5th Edition, (2012).
- Apar Gupta, Commentary on Information Technology Act, 3rd Edition, Lexis Nexis, 2016.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is E-Governance?

Electronic Governance or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back-office processes and interactions within the entire governmental framework. E-governance allows citizens to communicate with the government, participate in the governments' policy-making and citizens to communicate with each other.

2. What are the various types of E-governance?

The various types of e-governance are as follows:

i. Government-to-Citizen (G2C)
ii. Government-to-Business (G2B)
iii. Government-to-Employee (G2E)
iv. Government-to-Government (G2G)

3. What are the characteristics of Good Governance?

Good governance has 8 major characteristics. It is participatory, consensus-oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive and follows the rule of law. It assures that corruption is minimized, the views of minorities are taken into account and that the voices of the most vulnerable in society are heard in decision-making. It is also responsive to the present and future needs of society.

4. What are the objectives of E-Governance?

- To build an informed society
- To increase Government and Citizen Interaction
- To encourage citizen participation
- To bring transparency in the governing process
- To make the Government accountable
- To reduce the cost of Governance
- To reduce the reaction time of the Government

1.12 ACTIVITY

Explain the meaning of E-Governance, its features, objectives, types and how it is useful in the present era? (800 – 1000 words)

Unit 2: Legal Issues and Regulatory Framework of E-Governance

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Regulatory framework under I.T. Act, 2000

1.3 Some E-governance initiatives of the Indian Government

1.4 Issues involved in E-Governance

1.5 Challenges involved in E-Governance

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going this chapter, you should be able to understand:

- Regulatory Framework under I.T. Act, 2000
- Issues and Challenges involved in E-Governance
- E-Governance initiatives

1.2 REGULATORY FRAMEWORK UNDER I.T. ACT, 2000

Section 4-10 of the Information Technology Act, 2000 highlight the extent of e-governance rights to the individuals and to the Government.[92] The I.T. Act provides a road map for use of

[92] E-Government, E-Participation and Challenging Issues: <https://pdfs.semanticscholar.org/c8dc/0f2e99c6d798364ea55a43c10a3aea0ec174.pdf>

electronic records (including digital signatures) in Government and its agencies by promoting efficient delivery of Government services.[93]

I. LEGAL RECOGNITION OF ELECTRONIC RECORDS

Section 4 deals with Legal Recognition of electronic records.Where any law provides that information or any other matter shall be in writing or the typewritten or printed form, then irrespective of anything contained in such law, such requirement shall be deemed to be satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.[94]

II. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES

Section 5 relates to the Legal Recognition of electronic signatures.Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then irrespective of anything contained in such law, such requirement shall be deemed to be satisfied if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.[95]

'Signed', to a person, mean affixing of his handwritten signature or any mark on any document and the expression 'signature' shall be construed accordingly.[96]

III. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES IN GOVERNMENT AND ITS AGENCIES

[93](Gswan.gov.in, 2020)
<http://www.gswan.gov.in/PDF/D3-2-Regulatory-framework-of-e-Governance.pdf> accessed 20 May 2020.
[94]Electronic Governance | Ministry of Electronics
<https://meity.gov.in/content/electronic-governance>
[95]ICAI members use electronic signature for signing audit
<https://taxguru.in/chartered-accountant/icai-members-may-use-electronic-signature-signing-audit-reports.html>
[96]Chapter 3: Electronic Governance Archives - Page 2 of 3
<https://www.itlaw.in/bareact/chapter-3-electronic-governance/page/2/>

Section 6 deals with the use of electronic records and electronic signature in Government and agencies.

Where any law provides for:

- The filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner; or
- The use or grant of any licence, permit, sanction or approval by whatever name called in a particular manner; or
- The receipt or payment of money in a particular manner, then irrespective of anything contained in any other law for the time being in force, such requirement shall be deemed to be satisfied if such filing, issue, grant, receipt or payment is effected by means of such electronic form as may be prescribed by the appropriate government.
- The appropriate Government may, by rules, prescribe:
- The manner and format in which such electronic records shall be filed, created or issued;
- The manner or method of payment of any fee or charges for filing, creation, or issue any electronic record.

IV. DELIVERY OF SERVICES BY SERVICE PROVIDER

Section 6A pertains to the Delivery of Services by service providers.For the purposes of e-governance and efficient delivery of services to the public through electronic means the appropriate government may, by notification in the Official Gazette, authorize any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify.[97]

Service provider so authorized includes any individual, private agency, a private company, partnership firm, sole proprietor firm, or any other body or agency whichhas been granted permission by the appropriate government to offer services through electronic means in accordance with the policy governing such service sector.[98]

[97]<https://egovstandards.gov.in/sites/default/files/Guidelines/Digital%20Signature/Digital_Signature_Certificate_Interoperablity.pdf>

[98]E-Governance - Legal Bites <https://www.legalbites.in/e-governance/>

The appropriate government may also authorize any service provider to collect, retain and appropriate such service charges, as may be prescribed by the appropriate government for the purpose of providing such services, from the person availing such service.[99]

Further, the appropriate government may authorize the service provider to collect, retain and appropriate service charges even if there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers.

However, the appropriate government may specify the different scale of service charges for different types of services.

V. RETENTION OF ELECTRONIC RECORDS

Section 7 deals with Retention of electronic records.Where any law provides that documents, records or information shall be retained for any specified period, then that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form if:

- The information contained therein remains accessible so as to be usable for a subsequent reference;
- The electronic record is retained in the format in which it was originally generated, sent or received, or in the format which can be demonstrated to represent accurately the information originally generated, sent or received;
- The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

However, the above provision will not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Further, the above said provision shall not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

[99]INFORMATION TECHNOLOGY ACT, 2000 - Internet Rights <https://internetrights.in/wp-content/uploads/2014/05/Information-Technology-Act-2000.pdf>

VI. AUDIT OF DOCUMENTS ETC. MAINTAINED IN ELECTRONIC FORM

Section 7A pertains to Audit of Documents etc. in Electronic form.Where any law for the time being in force contains a provision for audit of documents, records or information, then such provision shall also be applicable for an audit of documents, records or information processed and maintained in the electronic form.

VII. PUBLICATION OF RULE, REGULATION ETC. IN ELECTRONIC GAZETTE

Section 8 deals with Publication of rule, regulation, etc., in Electronic Gazette.Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette.

- In ***Orissa Consumer Association Vs Orissa Electricity Regulatory Commission***[100]**,**the Orissa High Court held that "if notification is published in the Electronic Gazette, the notification shall be deemed to have been published in the Official Gazette".
- In ***Tirumala Devi EadaVs The State of Andhra Pradesh***[101]**,**it was held that on a reading of Section 8 together with Section 2(1) (s)[102] of the Act, it is clear that even where the law provides for publication in the Official Gazette, such requirement shall be deemed to have been satisfied if the Rules, Regulations, etc. are published in the electronic gazette i.e., in the electronic form.

VIII. NO RIGHT TO INSIST GOVERNMENT OFFICE ETC. TO INTERACT IN ELECTRONIC FORM

Section 9 talks about section 6, 7 and 8 to not confer the right to insist document should be accepted in electronic form.No right is conferred upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body

[100] *Orissa Consumer Association v Orissa Electricity Regulatory Commission* AIR [2005]Ori 11

[101] *Tirumala Devi Eada v The State of Andhra Pradesh*W P (C) Nos 34683, 34805 of [2011]

[102] Section 2(1) (s) of the I T Act, 2000, "Electronic Gazette" means the Official Gazette published in the electronic form

established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

IX. POWER TO MAKE RULES BY CENTRAL GOVERNMENT IN RESPECT OF ELECTRONIC SIGNATURE

Section 10 deals with the power to make rules by Central Government in respect of electronic signature.The Central Government may prescribe:

- The type of electronic signature;
- The manner and format in which electronic signature should be affixed;
- The manner or procedure which facilitates identification of the person affixing the electronic signature;
- Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
- Any other matter which is necessary to give legal effect to electronic signatures.

1.3 SOME E-GOVERNANCE INITIATIVES OF THE INDIAN GOVERNMENT

The Government of India approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 8 components in 2006. In the year 2011, 4 projects – Health, Education, PDS and Posts were introduced to make the list of 27 MMPs to 31. Currently, there are 44 MMPs being implemented by the government under e-Kranti.

Under Pillar 5 of Digital India, e-Kranti - Electronic delivery of services of Digital India programme, 44 Mission Mode Projects (MMPs) are being implemented by Central Ministries/Departments and State/UT governments to provide completely online services in various domains like Health, Education, Passport Seva, Trade, Income Tax, Excise and Customs, Corporate Affairs, India Post, e-Police, Land Records, etc. Several services are completely online, while some services are partially online.

INITIATIVES IN VARIOUS SECTORS

Agriculture: The major services of Agriculture MMP include Pesticide registration, Display on the Web of Seed Testing Results, Prices and arrival details, Geographical Information System (GIS) based interface for price and arrival details, District level Agro-met advisories, Information on pesticides, Information on fertilizers/seeds, etc.

SOME MAJOR MOBILE APPLICATIONS DEVELOPED ARE

KisanSuvidha: This app provides information on five critical parameters- weather, input dealers, market price, plant protection and expert advisories.

PushaKrishi: This app provides information on the latest technologies to farmers.

Crop Insurance: Famer can learn of insurance premium, notified area etc. on the mobile.

Agri Market: Farmer can learn about the prices of various crops in the mandis near him.

India Weather: This app provides current weather and 4 days of weather forecast across the country for more than 300 cities.

THE MAJOR WEB PORTALS DEVELOPED INCLUDE THE FOLLOWING[103]

Farmers' Portal: Farmers' Portal is a one-stop-shop for farmers where a farmer can get information on a range of topics including seeds, fertilizer, pesticides, credit, good practices, dealer network, and availability of inputs, beneficiary list and Agromet advisories.[104]

M-Kisan Portal: This is a unified platform from where officials and scientists can send targeted text and voice-based advisories to the farmers on a host of issues related to agriculture and allied sectors.

[103]'E-Governance In India: Concept, Initiatives And Issues - INSIGHTSIAS' (*INSIGHTSIAS*, 2020) <https://www.insightsonindia.com/2014/11/23/e-governance-india-concept-initiatives-issues/>

[104]Nikithayadav, Singh, V B (Sep.2012) -"e-Governance: past, present and future in India", international journal of computer applications (0975-8887) volume 53, No 7

Crop Insurance Portal: To provide complete information related to Crop Insurance scheme being implemented in the country.

Participatory Guarantee System of India (PGS) Portal: This is a portal for encouraging a participatory approach to certification of organic farming in the country.

E-Mandi: The Government has launched the e-Mandi portal to make procurement of agricultural products smoother and provide competitive remuneration, especially for small and marginal farmers.

Land Records: Major services include real-time availability of land records, issuance of Record of Rights along with cadastral maps, issuance of a certified copy of the deed, issuance of non-encumbrance certificate, payment of stamp duties etc. 26 States have computerized their land records and providing computerized copies of Records of Rights on demand. These states have also placed their land records data in the public domain.[105]

School Education Mission Mode Project (MMP): The MMP is focused on Primary, Secondary and Higher Secondary education. It will be a driving force for implementation of the National Policy on Information and Communication Technology (ICT) in School Education.

National Scholarships Portal (NSP): The portal is a one-stop solution to implement end-to-end disbursement of the scholarship to the beneficiaries. The process includes student registration, application, approval and disbursement. 76 schemes of 22 Ministries/ Departments of the Government are being on-boarded on the portal.

Aadhaar and Direct Benefit Transfer (DBT): 103+ crore citizens enrolled. 27+ Crore Bank Account seeded with Aadhaar No. 74 Government Schemes are on DBT, where Rs. 1.2 lakh crores transferred through DBT.

Central Excise and Customs: Facilitates trade and industry by streamlining and simplifying

[105](Meity.gov.in, 2020) <https://meity.gov.in/writereaddata/files/e-Governance_Project_Lifecycle_Participant_Handbook-5Day_CourseV1_20412.pdf> accessed 20 May 2020.

customs and excise processes and to create a climate for voluntary compliance.

MCA 21: The major services delivered under the aegis of Ministry of Corporate Affairs through MCA21 include viewing of public records, issue of certified copy of documents, change in registered office, change in director(s), annual filings, application for change of name of a company, incorporation of a company and name allocation to a new company.

Passport Seva: Project focuses on reforming Passport services in India through simple, efficient and transparent processes from the processing of Passport to delivery of services.

E-Tourist Visa: Tourists can apply visa online, pay the visa fee online and receive e-Tourist Visa online. Around 8.45 lakh e-Tourist Visas have been issued since November 2015.

E-Courts: The services delivered through the e-Courts MMP include Automated case filing, Automated registration of case, Automated workflow for court, Generation of automated cause list, Judicial service centers in all Courts, Automation of Case Management System, allocation of cases, etc.

Common Services Centers (CSC) 2.0: The CSC aims for establishing at least one CSC in each of 2.5 lakh Gram Panchayat (GP) level under Digital India Programme to deliver various G2C, B2C and B2B services online.

E-District: e-District services have been launched in 555 districts of the country, which delivers various types ofeGov services at districts.[106]

Mobile Governance: The Mobile Seva platform delivers Government services over mobile devices using mobile applications installed on the user's mobile handsets. About 2521 Government departments and agencies at central, state and local levels have been integrated with

[106] Kumar, Suneel (2016) -"e-governance in India, Imperial Journal of Interdisciplinary Research, volume.2, issue-2, issn: 2454- 1362

the Mobile Seva platform.

E-Hospital: Online Registration System (ORS): It includes online appointment and registration by new patients, viewing of lab reports, checking the status of blood availability and integration with payment gateway (PayGov). 43 hospitals have been integrated.

JeevanPramaan: Digital Life Certificate for Pensioners scheme known as JeevanPramaan envisages digitizing the whole process of securing the life certificate. With this initiative, the pensioner is no more required to physically present himself or herself in front of the disbursing agency or the certification authority. JeevanPramaan is a biometric enabled digital service for pensioners. 16.30 lakh pensioners registered for the scheme.

Vikaspedia: It is a multilingual collaborative content creation platform that promotes access and sharing of e-knowledge for the empowerment of underserved communities. Vikaspedia facilitates societal empowerment through provision of relevant information in various domains including Agriculture, Education, Health, Social Welfare, Energy and e-Governance in 22 scheduled languages of the country, besides English.[107]

MyGov: MyGov aims to establish a link between Government and Citizens towards meeting the goal of good governance. MyGov encourages citizens as well as people abroad to participate in various activities i.e. 'Do', 'Discuss', 'Poll', 'Talk', 'Blog', etc. There are multiple theme-based discussions on MyGov where a wide range of people can share their thoughts and ideas.

1.4 ISSUES INVOLVED IN E-GOVERNANCE

TECHNICAL ISSUES

1. Interoperability: It is one of the critical issues of e-governance. Interoperation among ministries and departments is difficult, and it became a hurdle for processing and sharing data. In other words, web-based data how to be captured and in which format these seem to

[107]Mahajan, Preeti (2009) E-Governance Initiatives in India with Special Reference to Punjab

be major issues of e-governance.[108]

2. Security: Nowadays, the security of online transaction is becoming a big issue; insurance, banking, utility bill payments, all these services done by e-governance. There is still discontent to citizens on availing government services due to lack of security.[109]

3. Privacy: This is another key issues of e-governance. Any information provided by citizens should be ensured by the government. Otherwise, any person or institution may misuse valuable information. 4. Authentication: It is very important to know the right user of the services, or it may be misused by private competitors. Meanwhile, the digital signature plays a major role in providing authenticity. It is expensive and causes for frequent maintenance.

ECONOMIC ISSUES

1. **Cost:** It is one of the economic issues, implementation of e-governance operations and maintenance of services fetch huge cost to govt.[110]

2. **Reusability:** Any models developed by the government, must be reusability. E-governance is being a national plan; what it incorporates any software or modules should be used by other administrations.[111]

3. **Maintainability:** Maintenance should be given due importance. Because the IT ministry has been continuously developing new softwares in order to fill the current needs of citizens. Consequently, the government launched new projects, for example, digital India.

[108]E-Governance in India: Issues and Challenges <https://pdfs.semanticscholar.org/b41a/d7d1537e49b90e40ec9b732736d6c16f3347.pdf>

[109]MeghashyamAthalyeShrinivas (Sep, 2013)-"e-Governance: issues and challenges", epitome: an online interdisplinary, multidisplinary journal, volume 2, issue 2

[110]Beniwal, V S, and Sikka, Kapil (2013) -"e-Governance in India: prospects and challenges, International Journal of Computer & Communication Technology, Issn: 0975-7449, volume-4, issue 3

[111] Malik, Poonam, Dhillan, Priyanka and Verma, Poonam. (July, 2014) -"Challenges and future prospects for E-governance in India", International Journal of Science, Engineering and Technology Research, volume-3, issue:7

4. **Portability:** The primary requisite for portable applications is the independence of components from hardware and software platforms in order to help in possible reuse by administrations.

SOCIAL ISSUES

1. **Accessibility:** In the era of technology, the most number of people using the internet via computers and mobile phones. In the context of India, there is still gap arising between users and nonusers; it is because of the language barrier, inadequate infrastructure in rural areas, etc.

2. **Usability:** Users of e-governance may be literate or illiterate. Any technology or software to be used as user-friendly to a greater extent; only then, citizens could use it as smoothly as possible.

3. **Use of local languages:** India's population is second next to china; over 65 % only literate citizens are there; the rest of the population cannot understand the English language. Therefore, the government should make it more comfort by translating this language into their regional languages for the sake of the benefit of e-services.

4. **Awareness about e-governance:** Number of people in the country has not been aware of it, on account of illiteracy, non-accessibility of the internet in rural areas, lack of will using internet services, etc. Therefore, educated citizens, concerned institution and department should come forward to get rural people benefited by e-services.

1.5 CHALLENGES INVOLVED IN E-GOVERNANCE

1. TRUST:

It is the emerging challenges of e-governance. Trust can be defined regarding users of new software and trust of the government. Former aspect implies that users of any type of software or technology must be confident, comfortable and trusting of it. Another very important aspect related to the trust of govt. Nowadays, citizens using e-governance services, trusting the innovations of e-governance to some extent.

Furthermore, there might be some fraudulent activities done by any other entity for the sake of finance, valuable info and even about personal information, etc. Besides, in Government offices, dept. valuable info sometimes left out or missed; it erodes trust about e-governance among all classes citizens of the economy.[112]

2. DIGITAL DIVIDE:

Even in the era of science and technology, there is still a huge gap that exists between users and nonusers of e-govt. services. In fact, in India, the majority of the masses, who live below the poverty line and they deprived of govt. services. In contrast, some portion of people is immensely using the e-services of government.However, this gap needs to be made narrow, then only,the benefits of e-governance would be utilized equally.[113]

3. COST:

One of the difficult tasks of the govt. is to spend on implementation of e-governance initiatives to which govt. has to bear the huge cost. Few other developed countries UK and Singapore spending 1% of GDP and 0.8% of GDP respectively. India spending only 3% of GDP, indeed, govt. should motivate the officials, administrators and common people using services of e-governance subject to the conscious use of public finance on these types of projects.[114]

4. PRIVACY AND SECURITY:

It is one of the critical challenges of e-governance. Financial services, medical services

[112]Paramashivaiah, P and Suresh, B K, E-Governance: Issues and Challenges in India (August 15, 2016) OIDA International Journal of Sustainable Development, Vol 09, No 08, pp. 11-16, 2016

[113]e-Governance in India : Empowering Citizens
<https://www.dhyeyaias.com/current-affairs/perfect-7-magazine/e-governance-in-india>

[114]Palanisamy, Ram (2004) Issues and challenges in e-governance planning

and personal information are to be protected with security, and then only, there will be a number of people trusting of it. Therefore, the implementation of e-governance projects must have security standard and protocols for safeguarding the interest of all classes of masses; otherwise, citizens will lose trust and confidentiality of e-governance.

5. INFRASTRUCTURE:

It is essentially required for the implementation of e-governance as much as possible in India. Electricity, internet and poor adaptability of technology will retard the progress of e-governance. In the context of developing countries, there should be enough basic facilities in order to give impetus to e-governance.

1.6 LET'S SUM UP

E-governance is getting momentous in India. E-governance has had a great role in each sphere of the economy over a number of years. India economy has been progressive one on account of good governance. Conventionally, the Government used to struggle to provide services to its citizens before initiatives of e-governance. When the government started launching many initiatives for e-governance; it has become one of the emerging economies due to its potentiality of ICT. Till now, government has implemented various initiatives with different projects (Digital India, e-kranti, etc.). However, it still has some hurdles regarding e-governance, such as digital divide between urban and rural, poverty, illiteracy, security and cost of implementation, etc. Each of these issues and challenges is posing a serious concern to the government. Meanwhile, previous and current govt. launched multiple initiatives by overcoming the above issues and challenges. Under twelve five year plan, some of the future prospects outlined and partly achieved by every government. However, the govt. should spend more on this initiative to make it transparent, convenient, and safer and citizen-friendly in order to enhance people confidence into good democratic e-governance.

1.7 FURTHER READING

- Tripathi, R., & Gupta, M. P. (2014). Evolution of government portals in India: mapping over stage models. Journal of Enterprise Information Management, 27(4), 449–474. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84927515542&partnerID=tZOtx3y1
- Chris Reed, Internet Law-Text and Materials, Universal Law Publishing Co., New Delhi, 2nd Edition, 2005.
- Ian J Lloyd, Information Technology Law, Oxford University Press, 7th Edition, 2014.
- AparnaViswanathan, Cyber Law Indian and International Perspectives, Lexis Nexis, 2012.
- Karnika Seth, Computers, Internet and New Technology Laws-A comprehensive reference work with special focus on developments in India. Lexis Nexis, Updated Edition 2013.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How has e-governance been legally acknowledged?**

   E-governance has been legally recognised through provisions of the Information Technology act 2000, such as sections 4 to 10 as laid down therein in the following manner.

   Section 4 – Legal Recognition of Electronic Records

   Section 5 – Legal Recognition of Electronic Signatures

   Section 6- Use of Electronic Records and Electronic Signature in Government and its Agencies

   Section 7- Retention of Electronic Records

   Section 8- Publication of Rules, Regulations, etc. in electronic gazette

   Section 9- Section 6, 7 and 8 to not confer the right to insist document to be accepted in electronic form

   Section 10 - Power to make rules by Central Government in respect of electronic signature.

2. Write any 5 Web Portals developed by the Indian Government?

- Farmers' Portal
- M-Kisan Portal
- Crop Insurance Portal
- E-Mandi
- Land Records

3. What are 3 legal issues involved in E-Governance?

- Technical issues
- Economic issues
- Social issues

4. What are the challenges involved in E-Governance?

- Trust
- Digital divide
- Cost
- Privacy and security
- Infrastructure

1.9 ACTIVITY

E-Governance in India: A Myth or Reality? (1500 words)

Unit 3: National E-Governance Plan (NeGP)

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Three tier architecture

1.4 The National E-Governance Plan (NeGP)

1.5 Approach/Methodology

1.6 Implementation strategy

1.7 Programme Management

1.8 Some Central Mission Mode Projects

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The meaning of National E-Governance Plan
- The Methodology and Implementation strategy of NeGP
- Some Central Mission Mode Projects

1.2 INTRODUCTION

India has a very strong presence in the IT sector globally, yet the benefits of the IT revolution have not truly percolated into the everyday life of the common man, particularly in rural areas. Experiments in IT-based service delivery has already been reaching heights. As mentioned earlier, some of them are e-Seva, and Bhoomi was more successful than the others. These early successes, as well as failures, showed that online services, served citizens better by reducing the burden of having to physically visit separate agencies, make contact with public officials, and be subjected to their discretion.[115]

NeGP is a major initiative of the Government of India, the first time under which a concerted effort is being made to take Information Technology to the masses in areas of concern to the common man. It aims to make most services available online, ensuring that all citizens would have access to them, thereby improving the quality of basic governance on an unprecedented scale.[116]

1.3 THREE TIER ARCHITECTURE

NeGP has a three-tier architecture. The **Common Service Centres (CSCs)** are the front-end delivery points for a range of citizen services. The common man feels empowered when he is able to get a service in a transparent manner, at a convenient location and an affordable cost. These centers also provide employment to the entrepreneurs running them, enumeration of data, insurance and IT education.

The second tier is of the common and support infrastructure that can allow information to be shared electronically between different agencies of the government and with citizens. Included in it, is the **State Wide Area Networks (SWANs),** which form the converged backbone network for data, voice and video throughout a State/UT and the **State Data Centers (SDCs)** which can provide common secure IT infrastructure to host state-level e-government applications and data.

[115]BhatnagarSubhash: "Unlocking E-Government Potentialconcepts, cases and practical Insights", Sage Publication, 2012

[116] Government of India, National E-Governance Plan, <http://india.gov.in/govt/national_egov_plan.php>

The third tier comprises the **27 Mission Mode Projects (MMPs)** which will transform high priority citizen services from their current manual delivery into e-delivery. Each MMP is owned and spearheaded by the relevant ministry/agency of the national government or by a state government, and is called **'mission mode'** because it has a definite timetable, service levels, project implementation team and process reengineering plans.[117]

1.4 THE NATIONAL E-GOVERNANCE PLAN (NeGP)

Over the past decade or so, there had been islands of e-Governance initiatives in the country at the National, State, district and even block level.[118] Some of them had been highly successful and were ready for replication across other States, while some have not produced the desired results or withstood the test of time. Experiences from successes as well as the failures of the various initiatives, played an important role in shaping the e-Governance strategy of the country. The basic lessons that emerged from the various e-Governance initiatives were:

- Need for political ownership at the highest level and a national vision for e-Governance for successful implementation of the programme;
- A dedicated team with a stable tenure from within the organization to conceptualize and implement the programme down the line;
- New areas of public-private partnership in making e-Governance possible should be continuously explored;
- Defined architecture, standards and policies addressing issues of security, privacy, etc.;
- An urgent need to develop the basic core and support infrastructure for e-Governance such as Data Centers, Wide Area Networks and the physical access points for delivery of government services, which would be common to all departments and where services could be delivered at the doorstep of the citizen in an integrated manner;
- Need to start with small pilots before scaling-up, as IT projects take a long time to implement, and often there are modifications to be incorporated along the way; and

[117] Administrative reform commission 11th report, chapter 7
[118] Common Service Centre: National E-Goveranance Plan (NeGP)
<https://upcsc.blogspot.com/2008/07/national-e-goveranance-plan-negp.html>

- Issues of re-engineering and management of change are of paramount importance in comparison to technical issues associated with e-Governance.

Hence, there was a felt need for taking a holistic view of the entire e-Governance initiative across the country. Increasingly, it was perceived that if e-Governance was to be speeded up across the various arms of government at the national, state and local government level, a programme approach would need to be adopted, which must be guided by a common vision, strategy and approach to objectives.[119] This approach would have the added advantage of enabling huge savings in cost, in terms of sharing the core and support infrastructure, enabling interoperability through standards etc., which would result in the citizen having a seamless view of Government. With this background, the National e-Governance Plan (NeGP) wasformulated by the Government, for implementation across the country.

[119]GuidlinesforOperational Model V4
<https://meity.gov.in/writereaddata/files/Guidlines_Operational_Model_V42_231210.pdf>

NeGPcomprises of 27 Mission Mode Projects (MMPs) to be implemented at the Central, State and Local Government levels and 8 Common Core and Support infrastructure.[120]

1.5 APPROACH/METHODOLOGY

The approach/methodology of NeGP encapsulates the learning from successes and failures of e-Governance initiatives across the country and the world, the recommendations/observations made by the Parliamentary Standing Committee and subsequently by the Committee of Secretaries (CoS).[121] The broad approach/methodology of NeGP is

- DIT would create ***Common and Support Infrastructure*** (State Wide Area Networks, State Data Centres, Common Service Centres, National/State Service Delivery Gateways)
- DIT would evolve/lay down ***Standards and Policy Guidelines, provide Technical and Handholding support, undertake Capacity Building, R&D*** etc. as required for successful implementation of various e-Governance projects.
- ***Mission Mode Projects (MMPs)*** would be owned and spearheaded by various concerned line Ministries. The Ministry/Department would be entirely responsible for all decisions connected with their MMP.
- States would be given the flexibility to identify a few ***additional state-specific projects (not exceeding 5)***, which are very relevant for the economic development of the State. In case, Central assistance is needed, such inclusions would be considered on the advice of the concerned Line Ministries/Departments.
- E-Governance would be promoted through a ***Centralized initiative[122]*** to the extent necessary to ensure citizen service orientation, to realize the objective of interoperability of various e-Governance applications and to ensure optimal utilization of ICT infrastructure/resources while allowing for and adopting, as a policy, a ***Decentralized Implementation Model.***

[120]<https://meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211(1).pdf>
[121] Article on Challenges and Future Prospects for E- Governance in India by PoonamMallick, PriyankaDhillon and PoonamVerma in 'International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 7, July 2014
[122]E Governance Initiatives in India
<https://www.thehansindia.com/posts/index/Hans/2016-02-01/E-Governance-Initiatives-in-India/204109>

- ***Successes would be identified, and replication promoted*** proactively with required customization.
- ***Public-Private Partnership (PPP)*** would be promoted wherever feasible to enlarge the resource pool without compromising on the security aspects.

1.6 IMPLEMENTATION STRATEGY

Implementation of the NeGP involves various Central Line Ministries/Departments and State Governments. Considering the multiplicity of agencies involved and the need for overall aggregation and integration at the national level, NeGP is being implemented as a programme, with well-defined roles &responsibilities of each involved agency

- Line Ministries/Departments are responsible for the implementation of the Mission Mode Projects (MMPs)/Components owned by them and work in a ***project mode within a tight, defined timeframe.***
- ***State Governments are responsible for implementing State Sector MMPs,*** under the overall guidance of respective Line Ministries in cases where Central Assistance is also required.
- ***DIT is the facilitator and catalyst for the implementation of NeGP*** and provides technical assistance to various Ministries and State Governments. In addition, it implements ***pilot/ infrastructure/ technical/ special projects and support components.***
- ***DAR&PG is responsible for Generic Process Re-engineering and Change Management,*** which are desired to be realized across all government departments. For various MMPs, concerned Line Ministries/ Implementing Agencies are primarily responsible for carrying out the required Process Re-engineering and Change Management.
- ***Planning Commission and Ministry of Finance allocate funds for NeGP*** through Plan and Non-plan budgetary provisions and lay down appropriate procedures in this regard.

1.7 PROGRAMME MANAGEMENT

For effective management of NeGP, a programme management structure has been created to accord credibility to the programme, to provide a forum to solicit view of stakeholders, to oversee the programme and resolve inter-ministerial/ inter-departmental issues and to ensure speedy sanctioning of projects.[123] The key components of the ***Programme Management*** structure are

- ***Cabinet Committee on Economic Affairs (CCEA)*** for programme level policy decisions.
- ***A body under the Chairpersonship of Prime Minister*** with representation drawn from relevant Ministries/ Departments, the National Knowledge Commission, the Planning Commission, experts, etc., to provide leadership, prescribe deliverables and milestones and monitor periodically the implementation of NeGP
- ***National e-Governance Advisory Group,*** headed by the Minister C&IT, to solicit views of external stakeholders and to provide inputs to the CCEA, advise the government on policy issues and strategic interventions necessary for accelerating the introduction of e-Governance across Central and State GovernmentMinistries/Departments.
- ***Apex Committee*** headed by the Cabinet Secretary to oversee the programme and to provide policy and strategic directions for its implementation. In addition, it moderates and drives services, process reengineering and service levels of each MMP wherever required. ***Further, it is empowered to add or delete MMPs as considered appropriate*** and to resolve all inter-ministerial issues. DIT acts as the Secretariat for
- ***Expenditure Finance Committee (EFC)/Committee on Non-Plan Expenditure (CNE)*** to financially appraise/ approve projects as per existing delegation of financial powers. The EFC/CNE headed by Secretary Expenditure would also be recommending to the CCEA the manner in which MMP Projects are to be implemented, i.e. as a Central Sector Scheme, Centrally Sponsored Scheme etc., as well as the financial terms of participation for States.
- Further, considering the complexity of the Programme and the need to look at issues such as overall technology architecture, framework, standards, security policy, funding strategy, service delivery mechanism, sharing of common infrastructure etc. at a program

[123]Paul, Anu& Paul, Varghese (2011) Project Management Model for e-Governance in the Context of Kerala State 191. 201-209. 10.1007/978-3-642-22714-1_22

level, ***the technical appraisal of all NeGP projects is done by DIT,*** prior to a project being placed before the EFC/ CNE.

- ***State-level Apex Committees*** headed by Chief Secretaries to allocate State level resources, set priority amongst projects and resolve inter-departmental issues.

1.8 MISSION MODE PROJECTS (MMPs)

NeGP consists of 27 Mission Mode Projects (MMPs) encompassing nine central MMPs, eleven state MMPs and seven integrated MMPs.[124] Line Ministries/Departments are responsible for the implementation of the assigned Mission Mode Projects (MMPs. Mission Mode Projects would be owned and spearheaded by various line Ministries for Central Government, State Governments and Integrated projects. Each department works in a project mode within a tight, defined timeframe by preparing a detailed project document, either in-house or with the assistance of a Consultant. This document spells out all important aspects of the project like services and service levels, project implementation team, process reengineering proposed, change management plan, project management plan, timelines, etc. The services and service levels are determined in consultation with the actual users.

State Governments are responsible for implementing State MMPs, under the overall guidance of respective Line Ministries in cases where Central Assistance is also required.

1.9 SOME CENTRAL MISSION MODE PROJECTS

1) MCA 21

The vision of the MCA21 project implemented by the Ministry of Corporate Affairs (MCA), Government of India, was ***"to introduce a service-oriented approach in the design and delivery of Government services".***[125]

[124]<www.mmp.cips.org.in/documents/workshops/2015/9- janeKranti.pdf>
[125]Central Mission Mode Projects ! - IAS OUR DREAM
<https://swapsushias.blogspot.com/2014/09/central-mission-mode-projects.html>

Its mission was ***"to build up a secure portal that offers the availability of all registry related services including the filing of documents, registration of companies and public access to corporate information. The portal services can be accessed/availed from anywhere, at any time that best suits the corporate entities, professionals and the public at large".***

The project will be integrated with the ***National e-Governance Services Delivery Gateway (NSDG),*** which will help extend MCA services to businesses via multiple front-end delivery channels, and which will also help provide other value-added services over and above the base services offered by MCA21.

There are more than 100 services covered within the scope of MCA21.

Among these, the major services are as follows:

- Name approval
- Incorporation of new companies
- Filing of Annual Statutory Returns
- Filing of forms for change of names/address/Director's details
- Creation/Modification/Satisfaction and verification of charges
- Filings for various statutory services required under the Companies Act
- Inspection of company documents (public records)
- Investor grievance Redressal

2) PENSIONS MISSION MODE PROJECT

The pensions MMP is primarily aimed at making the pension/retirement-related information, services and grievances handling mechanism accessible online to the needy pensioners, through a combination of interactive and non-interactive components, and thus, help bridge the gap between the Pensioners and the Government.

The portal provides the following services

- ***Online registration of grievances:*** These grievances are passed on to the Ministry/Department concerned online as well as through post for redressal.

- ***Dissemination of information*** concerning pension and retirement-related benefits to Pensioners, other Stakeholders, etc. All orders/instructions are uploaded on the Portal for the users.

As an additional facility, Utility services have also been made available to users on the Portal by establishing hyperlinks to the websites of some of the State Directorates of Pension and AGs of various States, though the Department has no role to play on State Government pensioners.[126]

3) INCOME TAX MISSION MODE PROJECT

The Income Tax Department of India is implementing a plan for setting up a comprehensive service that enables citizens to transact all businesses with the Department on an anywhere, anytime basis. Return of income for companies has to be filed compulsorily online every year.

OBJECTIVES

- ***Systems Integrator and Databases Migration & Consolidation:***
  Have a single ITD application running over a single national database with BCP and DRS.[127]
- ***PAN Module and PAN Related Services:*** Provide PAN card to citizens and improve authentication for all major financial transactions.
- ***Electronic filing of Income Tax Returns:*** To enable all taxpayers to fulfil their statutory obligation of filing their Income Tax Return electronically – 'Anytime', 'Anywhere', securely and conveniently using the Internet.
- ***Tax Information Network (TIN):*** Deliver more than 18 e-services to the taxpayers through digitization of all processes, filing of forms/applications, digitization of tax payments, authentications, tax credit verifications and refund processing. Many TIN services are disseminated through 1750 NSDL facilitation centres set up all over the country. TIN infrastructure also serves the ITD manpower and the Central Government in day to day monitoring of taxpayers data and in making informed policy decisions.

[126] International Journal of Science, Engineering and Technology Research (IJSETR) volume 3, Issue 7, July 2014
[127] CENTRAL MMPs.
<https://www.panchayatportals.gov.in/documents/4856434/0/CENTRAL%20MMPs.pdf>

- ***Refund Banker Scheme:*** Fast track issue of refunds through agency bank (SBI) and enable web-based tracking of refund status.

4) PASSPORT MISSION MODE PROJECT

The Consular, Passport and Visa (CPV) Division of the Ministry of External Affairs (MEA) provides passport and consular services to Indian citizens through the Central Passport Organization (CPO), and consular and visa services to foreign nationals and Indians residing overseas through the passport, visa and consular wings of over 160 Missions and Posts abroad. Various efforts by the CPO have led to significant improvement in productivity.

Despite all such measures, it was increasingly apparent that strategies adopted were proving inadequate to handle the growing demands on the Central Passport Organization. The quality of services provided to the citizens was being badly affected by the huge increase in workload without a concomitant increase in manpower and infrastructure. It was also evident that conventional solutions would not work in this situation.[128]

Thus, the Passport Seva Project was launched by the Ministry of External Affairs to redeem the situation by infusion of technology, process reengineering and staff motivation and commitment. The end objective being delivery of Passport Services to the citizens in a timely, transparent, more accessible, reliable manner & in a comfortable environment.

5) IVFRT MISSION MODE PROJECT

India has emerged as a key tourist destination, besides being a major business and service hub. Immigration Check Post is the first point of contact that generates public and popular perception about the country, thus necessitating a state of the art system for prompt and user-friendly services.[129]

Within the generic objective of facilitating legitimate travellers without compromising security, it is necessary to develop a secure, integrated service delivery framework to enhance security and facilitation in the Visa issuance process, and the Immigration function besides fortifying the Foreigners registration processes for effective tracking of foreigners. The Passport, Visa issuance

[128]'Mission Mode Projects | Welcome To Negd | National Egovernance Division (Negd)' (*Negd.gov.in*, 2020) <https://negd.gov.in/mission-mode-projects>

[129]Maurya, Ashutosh&Kar, Arpan (2014) Prioritising e-Governance Mission Mode Projects through systematic approaches

& consular matters, Immigration, Foreigners registration & tracking and Emigration, are inter-related subjects involving the Ministries of Home Affairs (MHA), External Affairs (MEA), Overseas Indian Affairs (MOIA), Central Board of Excise & Customs, and Civil Aviation. Many other Ministries in the Government of India (M/o Health and Family Welfare, M/o Tourism, M/o Commerce, etc.) also have a stake in this project.

The project for modernization and up-gradation of Immigration services is identified and included as one of the MMPs to be undertaken by the Ministry of Home Affairs under the National e-Governance Plan (NeGP). The MMP is titled ***"Immigration, Visa and Foreigners Registration & Tracking (IVFRT)".***

The project will be implemented across 169 Missions, 77 ICPs (Immigration Check Posts), 5 FRROs (Foreigners Regional Registration Offices), and FROs (Foreigners Registration Offices) in the State/District Headquarters.[130]

1.8 LET'S SUM UP

In this chapter, we have studied the meaning of National E-Governance Plan along with the three-tier architecture. We also studied the methodology and implementation strategy of NeGP. Finally, we ended the discussion on some Central Mission Mode Projects.

1.9 FURTHER READING

- Nazir, Mohsin&Wani, Sani&Arif, Tasleem. (2014). Current Scenario of the e-Governance Related Initiatives in India.
- Paul, Anu& Paul, Varghese. (2011). Challenges and Strategies of e-Governance in India. International Journal of Interdisciplinary Studies and Research: Baselius Researcher. XII. 472-480.

[130]<https://meity.gov.in/content/immigration-visa-and-foreigner%E2%80%99s-registration-tracking-ivfrt>

- E-governance in India: Concept, Initiatives and Issues - INSIGHTS, INSIGHTS (2019), https://www.insightsonindia.com/2014/11/23/e-governance-india-concept-initiatives-issues/

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What are the basic lessons that emerged from the various E-Governance initiatives?

The basic lessons that emerged from the various e-Governance initiatives were:

- Need for political ownership at the highest level and a national vision for e-Governance for successful implementation of the programme;
- A dedicated team with a stable tenure from within the organization to conceptualize and implement the programme down the line;
- New areas of public-private partnership in making e-Governance possible should be continuously explored;
- Defined architecture, standards and policies addressing issues of security, privacy, etc.;
- An urgent need to develop the basic core and support infrastructure for e-Governance such as Data Centers, Wide Area Networks and the physical access points for delivery of government services, which would be common to all departments and where services could be delivered at the doorstep of the citizen in an integrated manner;
- Need to start with small pilots before scaling-up, as IT projects take a long time to implement, and often there are modifications to be incorporated along the way; and
- Issues of re-engineering and management of change are of paramount importance in comparison to technical issues associated with e-Governance.

2) What is the three-tier architecture taken by Government of India?

- The Common Service Centres (CSCs)
- State Wide Area Networks (SWANs)
- 27 Mission Mode Projects (MMPs)

3) What are the major services under MCA21?

The major services are as follows:

- Name approval
- Incorporation of new companies
- Filing of Annual Statutory Returns
- Filing of forms for change of names/address/Director's details
- Creation/Modification/Satisfaction and verification of charges
- Filings for various statutory services required under the Companies Act
- Inspection of company documents (public records)
- Investor grievance Redressal

1.11 ACTIVITY

What is NeGP? Elucidate its approach, implementation strategy and programme management along with the few Central Mission Mode Projects? (1000 words)

Unit 4: Integrated and State Mission Mode Projects

4

SUBJECT CODE – PGDCL 102

E-COMMERCE, E-GOVERNANCE AND E-CONTRACT

BLOCK 2 – E-GOVERNANCE

UNIT 4 – INTEGRATED AND STATE MISSION MODE PROJECTS

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Integrated Mission Mode Projects
1.3 State Mission Mode Projects
1.4 Future of E-Governance
1.5 Let's sum up
1.6 Further reading
1.7 Check your progress: Possible answers
1.8 Activity

1.1 LEARNING OBJECTIVES

After going this chapter, you should be able to understand:

- The Integrated Mission Mode Projects
- State Mission Mode Projects
- Future of E-Governance

1.2 INTEGRATED MISSION MODE PROJECTS

S. No.	Projects	Nodal Ministry/Department
01	CSC	Department of Information Technology
02	e-Courts	Department of Justice
03	EDI	Department of Commerce
04	India Portal	Department of Information Technology & Department of Administrative Reforms & Public Grievances
05	NSDG	Department of Information Technology
06	e-Biz	Department of Industrial Policy and Promotion
07	e-Procurement	Department of Commerce

1) CSC MISSION MODE PROJECT

The Government of India's National e-Governance Plan has a clear vision: to deliver, and make accessible all Government, Social and Private Sector services in the areas of agriculture, health, education, entertainment,FMCG products, banking and financial services, utility payments, etc. to the citizens at an affordable cost.[131] With this intent, the Common Services Centres (CSCs) were conceptualized as the front end service delivery outlets enabling smooth and transparent governance at the village level. An unhindered citizen-centric leaning makes the CSC scheme a strategic cornerstone of the NeGP, and one of the key infrastructure pillars. In that respect, not many doubt that the CSC project is a huge opportunity to touch rural India like never before.

Under the scheme, over one lakh internet-enabled kiosks are being set up in the rural areas spread across more than 600,000 villages. One Kiosk is intended to serve a cluster of five to six villages. Classified under the integrated MMPs, the scheme got the approval of Government of India in September 2006 involving a total outlay of Rs. 5742 crore.[132]

IMPLEMENTATION FRAMEWORK

The implementation at three levels:

Level 1: A village-level entrepreneur (VLE - loosely analogous to a franchisee) sets up a CSC in the nodal village to provide service to rural consumers in a cluster of 5-6 surrounding villages.

[131]Awareness of Government Policies | AIITA <https://aiita.org/initiatives/awareness>

[132]Maurya, Ashutosh&Kar, Arpan (2014) Prioritising e-Governance Mission Mode Projects through systematic approaches

Level 2: The Service Center Agency (SCA - loosely analogous to a franchiser) is an operator which manages; trains and builds the VLE network across the district. An SCA can service one or more districts in a state with one district covering approximately 100-120 CSCs.

Level 3: The State Designated Agency (SDA) facilitates the implementation of the CSC scheme within the state. It is primarily responsible for providing policy, content, financial and other support to the SCAs in the state.[133]

2) E-COURTS MISSION MODE PROJECT

The e-Court Mission Mode Project (MMP) was conceptualized with a vision to transform the Indian Judiciary by making use of technology. The project had been developed, following the report submitted by the e-Committee under Supreme Court on national policy & action plan on implementation of information communication tools in Indian Judiciary.[134]

OBJECTIVES

E-Court, an integrated MMP, has a clear objective - to re-engineer processes and enhance judicial productivity both qualitatively and quantitatively to make the justice delivery system affordable, accessible, cost-effective, transparent and accountable.

The scope of the project is to develop, deliver, install and implement automated decision making and decision support system in courts all over the country. The e-Courts project entails ensuring of digital interconnectivity between all courts from the ***taluk*** level to the ***apex*** court.

POWER OF SERVICES

The e-Courts MMP will provide a range of services prominent amongst them being

[133]<https://meity.gov.in/content/mission-mode-projects>

[134]Bhatnagar, Subhash et al (2007) Center for e-Governance, Indian Institute of Management, Ahmedabad, Draft Report Impact Assessment Study Of E-Government Projects in India, DIT, India

S No	Service	Details
1	Automation of Case Management Processes	Case Filing, Scrutiny, Registration, Case Allocation, Court Proceedings, Details entry of a Case, Case Disposal & restoration, Transfer of Case etc
2	Provision of online services	Certified copies of orders and judgments, Case status, Calculation of court fees, Cause lists, Institution Registers, and Court Diaries
3	Establish information gateways between courts and government agencies	Information exchange with police, prisons, land records department, registration offices etc; distant production/examination of under trial and witnesses through videoconferencing
4	Creation of National Judicial Data Grid	Monitoring of pendency in the courts

3) E-TRADE MISSION MODE PROJECT

The integrated mission mode project, Electronic Trade (eTrade) was conceptualized to facilitate effective and efficient mode of transacting business in the area of foreign trade. The Department of Commerce is the nodal agency for the implementation of the eTrade project. The project is being pursued in trade regulatory and facilitating agencies like Customs, Ports, Airports, Directorate General of Foreign Trade (DGFT), Banks, respective Container Corporation of India (CONCOR), export promotion organizations etc., who also happen to be the community partners

of the project.[135] The community partners have developed their systems for internal processing. eTrade Project interconnects these community partners and enables them to exchange messages through the web or FTP.

The major activities of the project are expected to be completed by June 2011. The project is being implemented on a self-support basis, and the funds are being provided by participating agencies and departments.

The various trade regulatory and facilitating agencies, have established electronic interfaces between them as well as with the trading community to allow electronic delivery of services.

OBJECTIVES

The simple objectives of the eTradeproject are illustrated below:-

- to facilitate effective and efficient delivery of services
- to simplify procedures and to make procedures transparent
- to provide 24-hour access to users with their partners
- to reduce the transaction cost and time
- to introduce international standards and best practices

4) NATIONAL PORTAL OF INDIA MISSION MODE PROJECT

There are over 5000 websites on the internet of various Indian government entities that include Ministries, Departments, States/Union Territories, district administration, organizations. Citizens have to search and browse several websites to avail a service. The National Portal of India provides a single-window unified interface for over 5000 websites thereby reducing a lot of inconvenience to the citizens.[136] This portal acts as a logical front end to the e-governance initiatives under various central/state/UT government schemes and programmes. The National Portal has a long list of beneficiaries, which besides common citizen also includes government

[135]Heeks, R (2003), MosteGovernment-for-Development Projects Fail: How Can Risks be Reduced? Institute for Development Policy and Management, University of Manchester, UK
[136]INTEGRATED MMPs
<https://www.panchayatportals.gov.in/documents/4752980/0/INTEGRATED%20MMPs.pdf>

departments, the corporate sector, NRIs, national and international media and the general public across the world.[137]

The National Portal comes with unique features geared up to facilitate smooth access, enhanced quality of services and convenient single window access for a variety of Government information and services. It is the central repository of documents, forms, services, acts, announcements, contact directories, schemes and rules.

OBJECTIVES

The objectives of the India Portal MMP are

- To ***establish a one-point source*** for availability of information about any Government of India constituent, be it the Central Government Ministries, Departments, State/UT Governments, Districts, Panchayats or even organizations and affiliates, for the benefit of the citizens, businesses and other target audience.
- To ***facilitate launch/ implementation*** of various e-governance initiatives by the Indian Government.
- To ***emerge as a comprehensive one-stop-source*** of government information and ***service delivery through a unified interface.***
- To ***define the standards for publishing the information and electronic delivery of government information and services*** thus facilitating, unified, seamless and universal access for citizens of India from all walks of life and of various demographic profiles.
- To ***establish a platform for participation by the public in the process of governance.***

5) NATIONAL SERVICE DELIVERY GATEWAY (NSDG) MISSION MODE PROJECT

Under the National e-Governance Plan (NeGP), various e-Governance applications are being implemented in order to provide speedy deliveryof government services to the citizens at affordable costs.[138]

[137] National Knowledge Commission (2007), Government of India, New Concept Information Systems Publication., New Delhi

In order to realize the NeGP vision, it is imperative that the different departments in the Centre, States and Local Government cooperate, collaborate and integrate information across the various levels, domains and geographies. The National e-Governance Service Delivery Gateway (NSDG), standards based (IIP/IIS/IGIS) messaging switch, will enable this by providing seamless interoperability and exchange of data across heterogeneous applications of geographically dispersed departments.[139]

OBJECTIVES

The objectives of the NSDG are:-

- To act as a core infrastructure for achieving standards-based interoperability (IIP/IIS) between various e-Government applications implemented at various levels and geographically dispersed locations.
- To evolve Gateway messaging standards and build a government-owned Central Gateway based on these standards.
- To act as a catalyst in enabling the building of Standards-based e-Governance applications with Gateway as the middleware to ensure interoperability.
- To enable integration across Centre, State or Local Governments thereby enabling Integrated Service Delivery and a Service Oriented Architecture (SOA) leading to joined-up government.
- To help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations.
- Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework.
- Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.

---

[138]Hamner, M and Qazi, R U R (2009), "Expanding the Technology Acceptance Model to Examine Personal Computing Technology Utilization in Government Agencies in Developing Countries", Government Information Quarterly, Vol. 26 No. 1, pp. 128-136

[139]<https://meity.gov.in/content/nsdg>

- Enable transaction logging and time stamping for tracking of transactions and centralized control.
- Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware de-linking the backend from the front end.[140]

6) E-BIZ MISSION MODE PROJECT

The e-Biz Mission Mode Project, being executed by Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry, Government of India, was conceptualized with the Vision.[141]

"To transform the business environment in the country by providing efficient, convenient, transparent and integrated electronic services to investors, industries and business throughout the business life cycle".[142]

OBJECTIVE

Like any other technology-driven project, e-Biz too has a clear mandate of addressing several issues that will result in making the industry interactions with the Government smooth ´seeking approvals and permissions, reducing the points of contact between the business entities and the Government agencies, standardization of information, and reducing the burden of compliance.

- Facilitate a 'one-stop shop' for procuring all business licenses and permits.
- Eliminate the need to physically interface with regulatory authorities at various levels of governance.
- Become a source for accessing all information 24X7, with respect to starting up a business.
- Allow business units to file returns, pay taxes and submit compliances through a single interface.

[140] Wahid, F (2013), "Themes of Research on eGovernment in Developing Countries: Current map and future roadmap", in 46th Hawaii International Conference on System Sciences (HICSS), USA, 2013, HICSS, USA, pp 1743-1752

[141] Kerr, N L and Tindale, R S (2004),"Group performance and decision making",Annual Review of Psychology, Vol. 55, pp. 623-655

[142] <https://meity.gov.in/content/e-biz>

7) E-PROCUREMENT MISSION MODE PROJECT

Various studies have estimated that globally government procurement accounts for around 5-15% of the national GDP. The estimates for government procurement for India vary from 3.4% to 5.7% of the GDP. Therefore efficient practices in procurement of goods and services by government agencies is important from the perspective of lowering cost of procurement of goods and services, optimal delivery of public services, efficient allocation and use of public funds, fair opportunities for suppliers to compete for government contracts, encouraging good governance practices in procuring entities, reducing corruption, providing legal certainty to procurement procedures, ensuring transparency and thereby also attracting foreign investment and partnerships.

Ministry of Commerce & Industry (Department of Commerce) has been nominated as the Nodal Ministry for implementation of E-Government Procurement (e-GP) Mission Mode Projects (MMP). The stakeholders of e-GP MMP include Central Government Departments, State Government Departments, Public Sector Undertakings of Central and State Government, Autonomous Organizations of Central & State Government and vendors spread across the country and abroad namely, MNCs, SMEs and tiny units.[143]

VISION

The vision of the e-Procurement MMP is "To create a national initiative to implement procurement reforms, through the use of electronic Government procurement, so as to make public procurement in all Sectors more transparent and efficient".

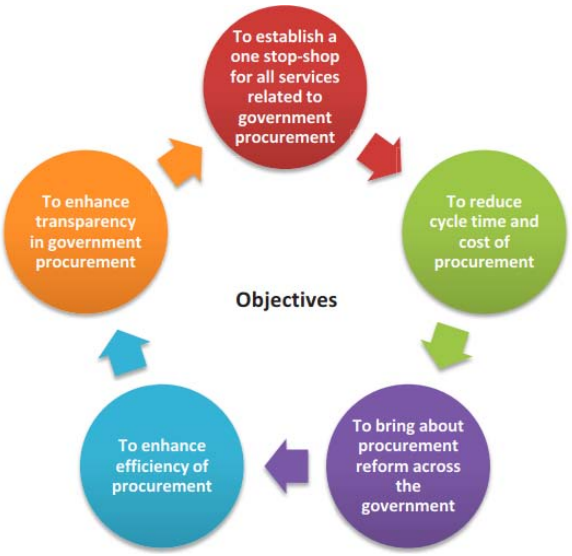
OBJECTIVES

The specific objectives of the e-Procurement MMP are to

- Establish a one-stop-shop providing all services related to governmentprocurement.
- Reduce cycle time and cost of procurement.
- Enhance transparency in government procurement.
- Enhance the efficiency of procurement.
- Bring about procurement reforms across the government.

[143]<https://meity.gov.in/content/e-procurement>

These objectives would be achieved through coordination and collaboration across the Government through the adoption of common standards.



1.3 STATE MISSION MODE PROJECTS

1) NLRMP MISSION MODE PROJECT

A Project for Computerisation of Land Records (CLR) was launched in 1988-89 with the intention to remove the inherent flaws in the manual system of maintenance and updation of Land Records. In 1997-98, the scheme was extended to tehsils to start distribution of Records of Rights to landowners on demand. The focus of the entire operation has always been to employ state of the art information technology (IT) to galvanize and transform the existing land records system of the country.[144]

The second important scheme, viz., ***Strengthening of Revenue Administration and Updating of Land Records (SRA&ULR)*** was launched in 1988-89 to help States and UTs in updating and maintaining the land records, setting up and strengthening of survey and settlement organisations and the survey training infrastructure, modernization of the survey and settlement operations and strengthening of the revenue machinery.

[144] <https://meity.gov.in/content/land-records>

However, the activities included in the schemes of CLR and SRA&ULR were basically meant for the strengthening of revenue administration although they also included activities that contribute to conclusive titling. The choice of activities was left to the States/UTs, most of whom chose activities that strengthen revenue administration but not necessarily helped in moving towards conclusive titling. A ***"hamper-of-activities"***was followed which led to eddying; and each activity became a goal in itself rather than a step in the systematic, ladder-like approach towards reaching the stage of conclusive titling. Moreover, the way the schemes have framed no timeframe for achieving the goal of conclusive titling could be set, and technology options for the survey were not indicated, and the work remained neglected in most of the States. Further, both the schemes excluded interconnectivity, geographic information system (GIS) mapping, connectivity with banks and treasuries and Registration - the last of which is a vital link in updating the land records.

Hence, the National Land Records Modernization Programme (NLRMP) was formulated by merging two Centrally-sponsored schemes CLR and SRA&ULR to usher in the system of conclusive titles as per the ***"Torrens System"*** with title guarantee in the country.

2) <u>ROAD TRANSPORT MISSION MODE PROJECT</u>

The Ministry of Road Transport & Highways has been facilitating the process of computerization of approximately 1000 Road Transport Offices (RTOs) across the country for the last 5 years.[145] Almost 90% of the RTOs have been computerized, and connectivity has been provided to 80% of the RTOs. Since the documents generated by the RTOs (Registration Certificate - RC & Driving License - DL) are valid across the country it was imperative to define the same standards for these documents on a pan-India level to ensure interoperability and correctness and timely availability of information. The SCOSTA committee was setup for this purpose and in addition to defining the Smart Card standards, had recommended uniform standardized software across the country, which has been designed and developed by NIC. The software namely **VAHAN** and **SARATHI** are being implemented across the country.

[145]<https://meity.gov.in/content/road-transport>

3) AGRICULTURE MISSION MODE PROJECT

Department of Agriculture and Cooperation (DAC) has over the years undertaken several IT initiatives such as AGMARKNET, SEEDNET, DACNET etc. Agriculture Mission Mode Project proposes to integrate these IT initiatives with the new applications/modules being developed as a part of the Project.[146]

Similarly, States / UTs have also either developed or are in the process of developing IT applications such as AGRISNET under various programmes of DAC. All such applications will be integrated with the Central Agri Portal (CAP), and the State Agri Portals (SAPs) envisaged under NeGP-A. The Central Agri Portal (CAP) and State Agri Portals (SAP) will also have the options of providing online feedbacks by the stakeholders. This would not only improve transparency but at the same time, would help in efficient monitoring.

4) CCTNS MISSION MODE PROJECT

The Crime and Criminal Tracking Network & Systems (CCTNS) Scheme has been approved by Cabinet Committee on Economic Affairs (CCEA)[147] in June 2009 with a provision of Rs 2000 Crores as a 100% Centrally Sponsored Scheme to be implemented during the remaining part of the 11th five year plan period (2009-2012).[148]

5) TREASURY COMPUTERIZATION MISSION MODE PROJECT

The State Treasuries are the structural and financial unit of the Government Financial System and are responsible for handling the day-to-day transactions of receipt and payment of Government. The functions generally performed by the treasuries are:-

- Receipt of Government Money
- Payments on behalf of Government
- Pension Payments
- Sale of Stamps through Vendors

[146]<https://meity.gov.in/content/agriculture>
[147]<https://meity.gov.in/content/police>
[148]E - Government Services India - Gujarat
<https://egovernmentservicesgujarat.blogspot.com/>

- Compilation of Government Accounts (District wise)
- Safe custody of valuables
- Maintenance of accounts for local fund/personal deposits etc.

1.4 FUTURE OF E-GOVERNANCE

Targets of the Twelfth Five Year Plan (2012-17) with respect to E-Governance[149]

1) A National Institute for E-Governance (NIG) would be setup as an autonomous State of the Art National Institute. NIG will also train at least 50 employees from Central Government per year on Project Management Certification.

2) An E-Governance Innovation and R&D Fund will be created to give adequate impetus to innovation in E-Governance and M-Governance.

3) Electronic Delivery of Services (EDS) Bill will be implemented. Assistance will be given to every Central Government Department in delivering at least one Service in electronic mode and every State Government in delivering at least three Services in electronic mode apart from the services which are already identified in the MMPs under NeGP.

4) Shared Services Platforms for e-Payment, GIS, call centre, etc. will be created.

5) An apps store will be created to promote the development of large scale E-Governance and M-Governance applications.

6) M-Governance platforms and frameworks will be created to enable the delivery of public services through mobile devices.

7) At least one person per family in 50% of the families will be targeted to provide basic IT training in the XII Plan period.

8) Cyber Security will be a major focus area during the Twelfth Five Year Plan Period.

9) Existing SWAN, SDC, NSDG/SSDG, India Portal, CSC Schemes will be rolled out and maintained in all States/UTs. These schemes would be further augmented and technologically upgraded.

[149]Report of the Working Group. Information Technology Sector <https://docplayer.net/16497521-Report-of-the-working-group-information-technology-sector-twelfth-five-year-plan-2012-17.html>

10) The e-District MMP will be implemented in all districts.

11) Training on Basic IT Skills will be introduced systematically for the existing and all new entrants into Government service.

1.5 LET'S SUM UP

In this chapter, we have studied the different integrated mission mode projects along with the various state mission mode projects. Finally we ended the discussion on the future of E-governance.

1.6 FURTHER READING

- Government of India, National E-Governance Plan, http://india.gov.in/govt/national_egov_plan.php.
- Office of the Registrar General & Census Commissioner, Census in India, Government of India, http://www.censusindia.gov.in/.
- Department of Information Technology, Industrial Promotion Division, Ministry of Communication & Information Technology, Government of India, http://www.mit.gov.in/default.aspx?id=243.

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) State the functions of Treasury computerization mission mode project?

- Receipt of Government Money
- Payments on behalf of Government
- Pension Payments
- Sale of Stamps through Vendors

- Compilation of Government Accounts (District wise)
- Safe custody of valuables
- Maintenance of accounts for local fund/personal deposits etc.

2) State two targets of 12th five year plan with respect to E-Governance?

- A National Institute for E-Governance (NIG) would be setup as an autonomous State of the Art National Institute. NIG will also train at least 50 employees from Central Government per year on Project Management Certification.
- An E-Governance Innovation and R&D Fund will be created to give adequate impetus to innovation in E-Governance and M-Governance.

3) What are the objectives of E-Procurement MMP?

- Establish a one-stop-shop providing all services related to governmentprocurement.
- Reduce cycle time and cost of procurement.
- Enhance transparency in government procurement.
- Enhance the efficiency of procurement.
- Bring about procurement reforms across the government.

1.8 ACTIVITY

Explain 5 integrated and State Mission Mode Projects along with its vision, objectives and functions? Enumerate the target of 12th five-year plan pertaining to e-governance? (1000-1500 words)

Block 3
E-Contract

Unit 1: Overview of E-Contract

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Concept of E-Contract

1.3 Essentials of Valid Contract vis-à-vis an E-Contract

1.4 Types of E-Contract

1.5 Difference Between Click-Wrap And Shrink Wrap Contracts

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- The concept of E-Contract
- Essential elements of E-contracts
- Different types of E-contracts

1.2 CONCEPT OF E-CONTRACT

E-contract is a kind of contracts formed by negotiation of two or more individuals through the useelectronic means, such as email, the interaction of an individual with an electronic agent, such

as a computer program orthe interaction of at least two electronic agents that are programmed to recognize the existence of a contract.[150]

E-contract is one of the divisions of e-commerce or e-business. It holds a similar meaning to traditional businesswherein goods and services are switched for a particular amount of consideration. The only extra element it has is that thecontract here takes place through a digital mode of communication like the internet. It provides an opportunity for thesellers to reach the end of the consumer directly without the involvement of the middlemen.[151]

E-Contracts are contracts attracting principles of *Uberrimaefidei* in which the contracting parties are not dealing atarm's length, but one party is entirely dependent upon the information supplied by the other party on the basis of whichalone he expresses his willingness to contract. The doctrine of *Uberrimaefidei* should be considered the foundation ofe-contracts as the chances of misrepresentation or suppression of material facts is most likely to occur in such transactions.

Although legal capacity is not explicitly dealt by the Information Technology Act, the law presumes that once an onlinecontract is concluded, both the parties are presumed to be competent to do so. In other words, neither party is allowed toraise an objection at a later stage that the contract is unenforceable for want of competence on the part of the parties.

The doctrine of *Uberrimaefidei* will be strictly adhered to in case of electronic contract, and one party acting to his detriment on the representation of the other that he is competent should not be put to any prejudice. E-contract is made through electronic mode with the help of internet. According to the mode of its formation, there are different types of electronic contracts. They are stated below.

1.3 ESSENTIAL OF VALID CONTRACT VIS-À-VIS AN E-CONTRACT

All the fundamental principles of contract law, have beendeveloped over the years through the judicial decisions of the courts apply to all contracts notwithstanding whether they are

[150]ELECTRONIC CONTRACTS IN INDIA: AN OVERVIEW <http://oaji.net/pdf.html?n=2017/488-1535975071.pdf>
[151]All About E-contracts- Meaning, Types and Law <https://taxguru.in/corporate-law/all-about-e-contracts-meaning-types-and-law.html>

formedelectronically, orally or through paper-based communications. Many of the issuesthat arise for consideration relate to how these conventional contract law principleswill apply to modem forms of technology. As in every other contract, an e-contractalso requires the following necessary elements:

OFFER

Like every other case, an offer is to be made to form an e-contract.In several transactions (whether online or conventional), however, theoffer is not made directly one-on-one. The consumer 'browses' theavailable goods and services displayed on the vendor's website and then'chooses' what he would like to purchase.

Under section 2(a) of The Indian Contract Act, speaks of offer. "When one person signifies his willingness to do or to abstain from doing anything with a view to obtainingthe assent of that other to such act or abstinence, he is said to make a proposal".[152]

Advertisement on the website may or may not constitute an offer as offer and invitation to treat are two distinct concepts. Being an offer to an unspecified person, it is probably an invitation to treat, unless a contrary intention is clearly expressed. The test is of intention whether by supplying the information, the person intends to be legally bound or not. When consumers respond through an e-mail or by filling in an online form, built into the web page, they make an offer. The seller can accept this offer either by express confirmation or by conduct. When dealing with business websites, it is important to establish whether the content of that business website amounts to an "offer" or merely an "invitation to treat". An invitation to treat is not capable of being turned into a binding contract by simply accepting its terms. Rather, it is an invitation to others to make an offer of their own. By contrast, an offer is an expression of willingness to enter into a binding contract with another party.[153]

The question which arises is, does it apply in electronic contracts? Is it when it enters the computer resource as provided under Section 13 of the IT Act or when the offeror receives an acknowledgement as in section 12 of the IT Act?

[152]E-contracts. Essentials, variety and legal issues <https://www.grin.com/document/427203>

[153]Sundaram, Sethuram&Deepa, Ms & Kumar,. (2018). E-Contracts in India: The Legal Framework, Issues and Challenges 4 13-15

It is clear that a message can enter into a person's mailbox without him seeing it. Thus, the element necessary for determining communication of offer in case of posts cannot be the same in electronic communication. The communication of offer is complete when it comes to the knowledge of the offeree and acknowledgement is received by him.

The offeror is able to revoke the offer any time before the communication of acceptance is complete as provided in section 5 of the Indian Contract Act and has not been altered by the IT Act.

ACCEPTANCE

The offer needs to be accepted. The acceptance is more oftenthan not undertaken by the business/ vendor after the offer has been madeby the consumer in response to the invitation to treat. The offer isrevocable at any point in time before the acceptance is made.[154]

Once an offer is accepted, a contract is concluded except the postal acceptance rule applies. The postal acceptance rule is an exception to the general rule that acceptance of a contract must be communicated to the offeror before a contract can be in existence. Under the rule, acceptance of a contract is said to occur at the time the acceptance is posted. Hence, the communication of acceptance is complete against the proposer when it is put in the course of transmission to him and as against the acceptor when it comes to the knowledge of the proposer, that is, when the acknowledgement enters into the designated computer resource. There is no disparity between Indian and Common law in this regard as seen in ***LalmanShukla v. GauriDutt Sharma***[155] where in spite of the fact that he found the boy whose uncle had promised Rs. 501 to anyone who finds was denied the reward seeing that he came to know only after finding the boy.

Both offer and acceptance can be generally done through email, website forms, and online agreements.

LAWFUL CONSIDERATION

[154] The Law of Contracts & Tenders with a Special Chapter on E-Contracts, T S VenatesaIyer's&, ed10th, S Gogia& Company, at p 106

[155] *LalmanShuklavGauriDutt Sharma*[1913] 40 ALJ 489

There has to be a lawful consideration. Anyagreement formed electronically, to be enforceable by law, must havea lawful consideration.[156]Consideration is oneof the most important elements of a contract. The basic rule is that when aparty to a contract promises to perform his promise, he must getsomething in return for the performance of his promise. Consideration issomething of some value in the eyes of the law.[157] It may be of some benefit,right, interest or profit given to the party as inducement of promise. Anact constituting consideration must be moved at the desire of thepromisor and must be legal, real and not imaginary. Promises that arephysically impossible to perform cannot have real consideration.

INTENTION TO CREATE LEGAL RELATIONS

There has to be an intention to createlegal relations. If there is no intention on the part of the parties to create legal relationships, then no contract is can be formed between them. By and the agreements of a domestic or social nature are notcontracts and are, therefore, not enforceable.

COMPETENCY OF THE PARTIES

All the parties to the contract must be lawfullycompetent to enter into a contract. Agreements entered into by incompetent persons, such as minors, lunatics, insolvents, etc. are void.Parties to a contract must be capable of enteringinto a contract. He must attain the age of majority and must be of soundmind. He must not be disqualified from contracting by any law for thetime being in force. In our country, an agreement where either party is aminor has no significance. It is considered a void ab-initio. As per section 12 of the Indian Contract Act, 1872, any person who is in aposition to judge and safeguard his interest is of sound mind andcapable enough to enter into a contract. When a person is declaredinsolvent by any competent Court, he cannot enter into a contractrelating to his property. In the old age foundation case of MohoriBibeevs.DharmodasGhose, (1903) 30 Cal. 539 it was held by the PrivyCouncil that an agreement by a minor is void.

FREE CONSENT

[156]<https://www.lawyersnjurists.com/article/consideration-important-elements-valid-contract/>
[157]<http://elib.bvuict.in/moodle/pluginfile.php/183/mod_resource/content/0/Advantages%20of%20EContracts%20over%20Traditional%20Contracts%20-%20E-Contracts%20and%20ECommerce%20in%20India%20-%20Vijaysinh%20Shashikant%20Pisal.pdf>

There must be free and genuine consent. Consent is said tobe free when it is not caused by coercion,misrepresentation, undue influence or fraud. In short, there must not be any subversion of the will of any party to thecontract to enter into such contract.[158] Generally, in online contracts, especially when there is no active interaction between thecontracting parties, e.g., between a website and the customer who buys through such a site, but the 'click-throughprocedure' ensures free and genuine consent.[159]

Consent which isdefined under Section 13 of the Indian Contract Act, 1872,[160] is an essentialrequirement of a contract. It is the meeting of minds of theparties. When both agree upon the same thing, in the same manner, theyare said to consent. In case consent is caused by coercion, it is voidableat the option of the party whose consent was so caused. Coercionincludes physical compulsion, threat, and violence. Consent has to befree and genuine and not induced by misrepresentation, undue influence.*e.*a case where one person is in a position to dominate the will ofanother. But in case of an online contract, there is a narrow scope ofphysical communication between the website and the customer availingtheir service; they give consent by clicking the option that ensuresfree and genuine consent.

LAWFUL OBJECT

The object of the contract must be lawful. A contractpresupposes lawfulness of the object of the contract. Therefore,anagreement for selling narcotic drugs or pornography films online is void.

CERTAINTY AND POSSIBILITY OF PERFORMANCE

There must be a certaintyand possibility of performance. A contract, to be enforceable, should notbe vague oruncertain or ambiguous; and there must be the possibility of itsperformance. A contract, which is impossible to perform, isvoid, e.g. where a website promises to sell land on the moon. Similarly, anagreement, the meaning of which is not certainor capable of being madecertain is to avoid.

[158]E- Contracts and the Law - Indian Law Watch <https://indianlawwatch.com/practice/e-contracts-and-the-law/>
[159]E- Contracts and the Law - Indian Law Watch <https://indianlawwatch.com/practice/e-contracts-and-the-law/>
[160] The Indian Contract Act, 1872, Dr Narender Kumar,1st ed 2015, Allahabad Law agency, at p 870-871

1.4 TYPES OF E-CONTRACT

1. E-MAIL CONTRACTS

Though e-mail communication has some of the trappings of instantaneous communication, nevertheless, it is a fragmented process involving many stages. The e-mail message is split into various packets and sent via different routes. Further, unlike in instantaneous forms of communication, the sender does not know if the transmission of the e-mail is successful, for even though he gets a delivery receipt, it only signals delivery to the mailbox and does not indicate that the other party has the knowledge of the receipt. Thus, e-mail messages would come under the category of the non-instantaneous form of communication. The default rules enunciated above would apply to e-mail contracts.[161]

2. STANDARD FORM OF E-CONTRACTS

The concept of contract as a freely negotiated bargain has received severe strains in the modern age of mass production, mass marketing and mass consumerism and transportation. One must admit that the consumer has very little economic strength to dictate the terms and conditions favourable to him in a contract. On the other hand, the manufacturer, whole seller, producer, a carrier and other big companies having giant economic strength are in a favourable position to dictate terms and conditions and the other party contracting with them are quiet unable to insist their terms. Consequently, these companies or producers etc. have drawn up standardised forms of contracts which are also known as adhesion.E-contracts are standard forms of contracts. Instead of using a printed paper, they are entered into an electronic mode. A standard form of contract is a contract prepared by one party to it, otherwise, than by process of negotiation drafted by one party it enables the other party, to sign on dotted lines. The terms are prepared beforehand by the former, and the latter party is made to or deemed to agree to the terms where under the latter does not have much say. The

[161] Pollock and Mulla Indian Contract Act and Specific Relief Acts, Mr R G padia, 13th ed 2006, Lexus Nexus ButterworthsWadhawa, Nagpur at p 153

terms are put a standardized form.[162]

The standard form of E-contracts can be broadly categorized into three types:
Click Wrap Contracts, ShrinkWrap Contracts and Browse Wrap Contracts

1. CLICK-WRAP CONTRACTS

A clickwrap agreement is mostly found as part of the installation process ofsoftware packages.[163] It is also known as "click-through" agreement or clickwraplicense. Click-wrap agreements allow "a buyer to manifest assent to the terms ofa contract by clicking on an acceptance button that appears while the buyerobtains or installs the product." A buyer cannot start using the software untilhe or she has clicked on the button accepting the terms and conditions of theagreement. Click-wrap agreements require buyer action in order to begin usagebut do not guarantee cognizance of the agreement terms. Buyers can assent tothe contract without even reading it in order to use the product. Buyers cannotnegotiate and must, therefore, accept the terms as they are. Most courts findthese agreements enforceable. Understandably, concern remains that click-wrapagreements may be accepted without users reading or understanding contract terms when manifesting assent. Click-wrap agreements can be of thefollowing types:

- Type and Click where the user must type "I accept" or other specifiedwords in an on-screen box and then click a "Submit" or similar button.This displays acceptance of the terms of the contract. A user cannotproceed to download or view the target information without followingthese steps.[164]
- Icon Clicking where the user must click on an "OK" or "I agree" buttonon a dialog box or pop-up window. A user indicates rejection byclicking "Cancel" or closing the window.

2. SHRINK-WRAP CONTRACTS

[162]Ilobinso, Ihuoma (2018) Formation of Electronic Contracts: Melding the Traditional Contract Law with Contemporary Electronic Commerce Citation Information
[163]Sneha J Joshi, A Study of Challenges and Benefits of Electronic Commerce, IMPACT: International Journal of Research inHumanities, Arts and Literature (IMPACT: IJRHAL), Volume 6, Issue 8, August 2018, pp. 25-32
[164] Alan Davidson, The Law o f Electronic Commerce (Port Melbourne: Cambridge University Press, 2009), atp 73

Shrinkwrap contracts are license agreements or other terms and conditionswhich can only be read and accepted by the consumer after opening the product. The term describes the shrink wrap plastic wrapping used to coat softwareboxes, though these contracts are not limited to the software industry. Shrinkwrap agreements operate slightly differently. For example, they have used whenone purchases off-the-shelf software. The agreement is imprinted on thesoftware box, CD-ROM case, or other materials included inside the package."The license begins when the purchaser reads its terms and tears open thecellophane wrapping or shrink-wrap that surrounds the package." Buyers aresupposed to return the software package to the retailer if they elect not to abideby the agreement. Courts are similarly concerned about buyers actuallyreceiving notice of the sale, consciously agreeing to the sale, and conditioningthe sale on acceptance of the license.

3. BROWSE WRAP AGREEMENT

This agreement is considered as a browsewrap agreement that's supposed to bebinding upon the contracting party with the aid of the usage of the website. Those encompass the consumer policies and phrases of service of websites alongwith Flipkart or E-bay and are in the shape of a "terms of use", a "personsettlement" or "terms of service", which can be used because of the hyperlinks atthe corner or backside of website.[165]

1.5 DIFFERENCE BETWEEN CLICK-WRAP AND SHRINK WRAP CONTRACTS

Basis	Click-wrap	Shrink-wrap
Knowledge of Terms and Conditions	**Consumer gets an opportunity to have a clear**	**Consumer does not get to know the key terms of the**

[165]Purohit, TD, "Contracts Via E-mail -A Note of Caution", Corporate Law Cases, Vol. 9, Part-11, 2008 (November), pp 488-489

	knowledge about the terms and conditions.[166]	**agreement.**
Acceptance and Agreement	**Allows the users to read the terms of the agreement before accepting them.**	**People agree to the terms by using the software which they have already purchased.**
Enforceability	**They have gained almost universal acceptance as law binding contracts.**	**They have questionable enforceability.**
Conclusion of Contract	**By clicking the 'accept' button.**	**By breaking the seal of the software bought.**

1.6 LET'S SUM UP

Electronic contracts simplify daily transactions for an e-consumer to a large extent.However, they also give rise to issues of free consent and freedom to contract. In this chapter, we have studied the concept of E-contracts, along with the essential elements of a valid contract. Finally, we ended the discussion with the different types of E-Contracts and their differences.

1.7 FURTHER READING

- David G Post & Dawn C, Nunziato, 'Shrink-wrap Licenses and the licensing on the Internet', Technology Licensing and Litigation (1997), at p- 519.
- The Indian Contract Act Sale ofGoods Act, Trikamal R. Desai, Lexis Nexis Butter worthsWadhava Nagpur, 20th Ed.at p-64.
- Sundaram, Sethuram&Deepa, Ms& Kumar,. (2018). E-Contracts in India: The Legal

[166]Shnikat, Morad&Alzubi, Ali &Aljaber, Maher &Alnsoor, Ali.(2017). THE LEGAL FRAMEWORK OF ELECTRONIC CONTRACT IN THE JORDANIAN LEGISLATION.Global Journal of Politics and Law Research. 5. 46-62

Framework, Issues and Challenges. 4. 13-15.

1.8 CHECK YOUR PROGRESS: POSSIBLE READING

1. **What is an E-Contract?**

It is an electronic contract, conceptually similar to traditional contracts albeit with a comparatively bigger realm and formed in the course of e-commerce and signed in electronic form without the use of paper or hard copies.

2. **What are the essential elements of a valid contract?**

- Offer
- Acceptance
- Lawful Consideration
- Intention to create legal relations
- Competency of the Parties
- Free consent
- Lawful Object
- Certainty and Possibility of Performance

3. **How many kinds of E-Contracts are there? Name them.**

There are three kinds e-contracts; click-wrap contracts, shrink-wrap contracts and browse-wrap agreements.

1.9 ACTIVITY

Explain the meaning of E-Contract, its essential elements along with the different types of E-Contracts? (1000 words)

Unit 2: Major Issues and Regulatory Framework of E-Contracts

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Laws that define E-Contracts

1.4 Regulatory framework under the I.T. Act, 2000 and other laws

1.5 Evidentiary value of E-Contract

1.6 Standard Form Online Contracts are unconscionable

1.7 E-Contracts and Consumer Protection

1.8 Major issues and challenges

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- The definition given by varied laws for E-contracts
- Regulatory Framework under I.T. Act, 2000 and other laws
- Major issues and challenges

1.2 INTRODUCTION

Since the last decade, there has been a tremendous technologyrevolution. Internet and transactions over the internet havebecome the sine qua non of everyday transactions throughoutthe world.[167] This is because of the emergence of informationtechnology-based economy.The World Wide Web (WWW) has brought new opportunities and challenges to variouspeople. The businesses utilize it for their benefit by expending their activities not only inphysical space but also in virtual space in search of potential customers. Thuscontracting becomes a fundamental element in the e-commerce world.[168] The electronic contracting raises various new legal issues. The advent of the Internet has changed the mode of entering intoan agreement, but the essentials of a valid contract are one andthe same. In India, the rules relating to the formation of contracts,its validity and enforcement are regulated by the Indian ContractAct 1872. However, there still remain some dark areas in theinterpretation of these contracts for which a consolidated lawgoverning e-contracts is required. The general inclination of the legislature andthe legal profession is to apply the existing law to the new sets of virtual commerceproblems without much change; even where modification is necessary or unavoidable toprotect the interest of e-businesses and e-consumers.

1.3 LAWS THAT DEFINE E-CONTRACTS

The UNCITRAL Model Law on E-commerce states that "a contract can be made by exchanging data messages; and when a data message is used in the formation of a contract, the validity of such contract should not be denied.[169]

The Information Technology Act, 2000, defines 'data' as a representation of information, knowledge, facts,[170] concepts or instructions which are prepared or have been prepared in a formalized manner, and are intended to be processed, are being processed or have been processed in a computer system or a computer network, and may, in any form (including

[167]Agbozo, Ebenezer. "Developing a Digital Government Framework for Sub-Saharan Africa" European Conference on Digital Government, Academic Conferences International Limited, June 2017, p 294
[168]ELECTRONIC CONTRACT AND THE LEGAL ENVIRONMENT <http://www.irfd.org/events/wf2003/vc/papers/papers_global/R38.pdf>
[169]Article 11, communication of data messages, UNICITRAL Model Law on E-Commerce, 1996
[170]STAMP DUTY IMPLICATIONS ON E-AGREEMENTS – Vinod Kothari <http://vinodkothari.com/2020/01/stamp-duty-implications-on-e-agreements/>

computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.[171]

As per UNCITRAL Model Law, 'data messages' means 'information generated, sent, received or stored by electronic, optical or similar means including, but not limited to Electronic Data Interchange(EDI), electronic mail, telegram, telex or telecopy'.[172]

1.4 REGULATORY FRAMEWORK UNDER THE I.T. ACT, 2000 AND OTHER LAWS

- **INDIAN CONTRACT ACT, 1872**

The Indian Contract Act, 1872 governs the manner in which contracts are made and performed in India.[173] Every e-contract must comply with the provisions of the act to make it legally enforceable. In the context of contract formation, the parties to the contract can express it by means of data messages or electronic record. Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that data messages were used for that purpose.

- **INFORMATION TECHNOLOGY ACT**

E-contracts are considered to be valid under the IT Act, 2000. Under the IT Act, any information which is in writing, typewritten or printed form is made available to a user in the electronic form for subsequent reference shall be deemed to have satisfied the requirement of law.[174] The IT Amendment Act, 2008 clearly states that the validity of contracts through electronic means, 'Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic forms or means was

[171]Section 2(o) of Information Technology Act, 2000
[172]Article 2(a) of UNCITRAL Model Law on E-Commerce, 1996
[173]Electronic Contracts in India | E- Contract | <https://legalconclave.com/blog/electronic-contracts/>
[174] Section 4 of Information Technology Act, 2000

used for that purpose'.[175] Additionally, the Act lays down that the instruments to which the Information Technology Act, 2000 does not apply shall include negotiable instruments, power of attorney, a trust deed, a will and contracts for sale or transfer of Immovable Property.[176]

- **INDIAN EVIDENCE ACT, 1872**

The emergence of information and communication witnessed a drastic change by elevating the status of evidence recorded, generated or stored electronically from the secondary to primary evidential status. The evidentiary value of e-contracts is well-defined under Sections 85A, 85B, 85C, 88A and 90A of the Indian Evidence Act, which deals with the presumptions as to electronic records. Section 65A of the said act relates to the admissibility of the electronic record.

1.5 EVIDENTIARY VALUE OF E-CONTRACT

The Delhi High Court in ***Societe Des Products Nestle S.A. And Anr.Vs. Essar Industries andOrs***.[177]noted that "Rapid rise in the field of information and technology in the last decade of 20th Century and the increasing reliance placed upon electronic record by the world at large necessitated the laying down of a law relating to admissibility and proof of electronic record.[178] The legislature responded to the crying need of the day by inserting into the Evidence Act Sections 65A and 65B, relating to admissibility of computer-generated evidence in the only practical way it could so as to eliminate the challenge to electronic evidence. By virtue of the provisions of Section 65A, the contents of electronic records may be proved in evidence by the parties in accordance with the provisions of Section 65B." Section 65B of the Indian Evidence Act, 1872 ("Evidence Act"), provides for the admissibility of electronic records. Any information contained in an electronic record which is printed on a paper or

[175] Section 10A of the Information Technology (Amendment) Act, 2008
[176] Section 9 of the Information Technology (Amendment) Act, 2008
[177] *Societe Des Products Nestle S A And Anr vEssar Industries and Ors*[2006] (33) PTC 469 Del
[178] Newslex: March 2013 - Manupatra <https://www.manupatrafast.in/NewsletterArchives/listing/Newslex%20DHLaw/2013/Resources_%20Newslex%20-%20March%202013%20-%20D.%20H.pdf>

stored/recorded/copied on optical/magnetic media produced by a computer shall be deemed to be a document. Further, such document is admissible as evidence in any proceeding without further proof of the original, if the conditions laid down under the Evidence Actare satisfied. The observations of the Supreme Court in the case of ***State (N.C.T. of Delhi) vsNavjotSandhu @ AfsanGuru***[179]may be relevant in this regard. Further, while analysing the evidentiary value of electronic records including electronic signatures, the Delhi High Court in the ***State of Delhi v. Mohd. Afzal&Others***[180]held that"Electronic records are admissible as evidence. If someone challenges the accuracy of computer evidence or electronic record on the grounds of misuse of the system or operating failure or interpolation, then the person challenging it must prove the same beyond reasonable doubt." Also, the Supreme Court in ***State of Punjab &Ors. Vs. M/S. Amritsar Beverages Ltd. &Ors***[181] while referring to the recent amendments on account of internet and other information technologies observed that "Section 464 of the Indian Penal Code deals with the inclusion of the digital signatures. Sections 29, 167, 172, 192 and 463 of the Indian Penal Code have been amended to include electronics documents within the definition of 'documents'. Section 63 of the Evidence Act has been amended to include the admissibility of computer outputs in the media, paper, optical or magnetic form. Section 73A prescribes procedures for verification of digital signatures. Sections 85A and 85B of the Evidence Act raise a presumption as regards electronic contracts, electronic records, digital signature certificates and electronic messages." As also appreciated by the Supreme Court of India, certain statutory amendments have been carried out in order to keep pace with technologies and further to align the existing set of laws with the IT Act, thereby opening the doors of the judicial system for admission of such electronic records. Further, in addition, meeting the prerequisites of a valid contract under the Contract Act, courts around the world have opined that for electronic contracts to be valid, the following additional requirements are to be satisfied:

- Clear notice to the customer that the transaction is governed by the terms of a contract;
- An opportunity to review the terms of the standard form contract before agreeing to them; and

[179]*State (N.C.T. of Delhi) v NavjotSandhu @ AfsanGuru* AIR [2005] SC 3820
[180]*State of Delhi v MohdAfzal&Others*107 [2003] DLT 285
[181]*State of Punjab &Ors v M/S Amritsar Beverages Ltd&Ors* AIR [2006] SC 2820

- A clear and unambiguous statement of what constitutes acceptance of the terms of the contract.

These requirements are in addition to the standard contract requirement for a signature or other act of assent (e.g., clicking on an "I Accept" button or by checking the box provided in the website).

The evidentiary value of e-contracts can be well understood in light of the following sections of the Indian Evidence Act. Sections 85A, 85B, 88A, 90A and 85C deals with the presumptions as to electronic records whereas Section 65B relates to the admissibility of an electronic record.

THE ABOVE MENTIONED SECTIONS CAN BE EXPLAINED AS FOLLOWS:

SECTION 85A:

As regards presumption to electronic agreements, this section is incorporated. It says that every electronic record of the nature of an agreement is concluded as soon as a digital signature is affixed to the record. Section 85A has been added in order to ensure the validity of e-contracts. But there are some restrictions as regards the presumptive value. The presumption is only valid to electronic records, electronic records that are five years old and electronic messages that fall within the ambit of Section 85B, Section 88A and Section 90A of Indian Evidence Act.[182]

SECTION 85B:

Section 85B provides that the court shall presume the fact that the record in question has not been put to any alteration, in case the contrary has not been proved. The secure status of the record may be demanded until a specific time. The digital signature should also be presumed to have been affixed with the intention of signing and approving the electronic record. Further, it has been provided that the section should not be misread so as to create any presumption relating to the integrity or authenticity of the electronic record or digital signature in question.

SECTION 88A:

"The court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed

[182]Evidentiary Value of E-Contracts - Legal Service India.
<http://www.legalserviceindia.com/article/l127-E-Contracts.html>

corresponds with the message as fed into his computer for transmission, but the court shall not make any presumption as to the person by whom such message was sent".[183]

This section is self-explanatory as it purports to follow the basic rules of a valid hard-copy agreement. The words "may presume" authorize the court to use its discretionary power as regards presumption. Sections 85A and 85B contained the words "shall presume" which expressly excluded this discretionary power of the court.

SECTION 90A:

In case of an electronic record being five years old, if proved to be in proper custody, the court may presume that the digital signature was affixed so as to authenticate the validity of that agreement. The digital signature can also be affixed by any person authorized to do so. For the purpose of this section, electronic records are said to be in proper custody if they are in the custody of the person with whom they naturally be. An exception can be effected in case circumstances of a particular case render its origin probable.

SECTION 85C:

As far as a digital signature certificate is concerned, the court shall presume that the information listed in the certificate is true and correct. Inclusion of the words "shall presume" again relates to the expressed exclusion of the discretionary power of the court.[184]

SECTION 65B:

Section 65B talks about the admissibility of electronic records. It says that any information contained in an electronic record which is printed on a paper or stored/recorded/copied on optical/magnetic media produced by a computer shall be deemed to be a document and is admissible as evidence in any proceeding without further proof of the original, in case the following conditions are satisfied:

[183] J H Grahams Smith, Internet Law and Regulation, Sweet and Maxwell, New Delhi, 2007, pp 773-775

[184] SarabdeenJawahitha, Noor RaihanAb Hamid, "Electronic Contract and The Legal Environment", available at: <http:// www.irfd.org/events/wf2003/papers_global/ R38.pdf>

The computer output was produced during the period over which the computer was used regularly to store or process information by a person having lawful control over the use of the computer. In case a combination of computers, different computers or different combinations of computers are used over that period, all the computers used are deemed to be one single computer.[185]

The information contained should have been regularly fed into the computer, during that period, in the ordinary course of activities. The computer was operating properly during that period, and if not, it would not have affected the accuracy of data entered.A certificate issued is also admissible if it contains a statement which:

- Identifies the electronic record containing the statement.
- Gives information about the particulars of the computer involved in the production of the record.
- The certificate issued should be signed by a person officially responsible for the use of that device in relation to the relevant activity. The information fed into the computer should be in the appropriate form as well as by appropriate device.

1.6 STANDARD FORM ONLINE CONTRACTS ARE UNCONSCIONABLE

Under e-contracts, there is little or no scope for negotiations to take place between the e-commerce platforms and the customers pertaining to the terms of the online contracts. The question that arises is whether such standard form contracts are to be considered unconscionable and may be struck down by the courts. Indian laws and Indian courts have dealt with instances where terms of contracts (including standard form contracts) were negotiated between parties in unequal bargaining positions. Under Indian Contract Act, if a person who is in a position to dominate the will of another, enters into a contract with him, and the transaction appears to be unconscionable, the burden of proving that such contract was not induced by undue influence

[185] Jeffery E. Wittmann ,Vancouver, BC. "Electronic Contracts", Negotiation and Drafting Major Business Agreements Conference Federated Press (October, 2007)
<http:// www. wdwlaw.ca/ELECTRONIC_CONTRACTS_111007_280312.pdf>

shall lie upon the person in a position to dominate the will of the other. [186] In addition to that, the consideration or object of any agreement is unlawful when[187]

- It is forbidden by law; or
- Is of such a nature that if permitted, it would defeat the provisions of any law; or
- Is fraudulent; or
- Involves or implies injury to the person or property of another; or
- The Court regards it as immoral or opposed to public policy.

In the case of ***LIC India Vs Consumer Education & Research Center[188],***the Supreme Court interpreted an insurance policy issued by Life Insurance Corporation of India by bringing in certain elements of public purpose. The Court held that certain clauses in the policy with regard to restricting the benefit of the policy only to those people employed in the Government as void under Article 14 of the Constitution of India, i.e., equality before the law.[189] The Court noted that 'In dotted line contracts, there would be no occasion for a weaker party to bargain as to assume to have equal bargaining power. He has either to accept or leave the service or goods on terms of the dotted line contract. His option would be either to accept the unreasonable or unfair terms or forgo the service forever'.

In the case of ***Lily White Vs R Munuswami[190],*** the court held that a limitation of liability clause printed on the back of a bill issued by a laundry which restricted the liability of the laundry to 50% of the market price of the goods in case of loss was against public policy and therefore void.

1.7 E-CONTRACTS AND CONSUMER PROTECTION

In E-contracts, the dominant party stipulates the terms and conditions in order to absolve itself from the liability. This has given rise to issues with regard to consumer protection. Subsequent to the Consumer Protection Act being passed in 1986, the trading system changed drastically. This Act had lacunas for modern consumer protection. There were many changes brought under the

[186] Section 16(3) of the Indian Contract Act, 1872
[187] Section 23 of the Indian Contract Act, 1872
[188] *LIC India v Consumer Education & Research Center*[1995] AIR 1811
[189] Article 14 of Indian Constitution states that, the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India
[190] *Lily White v R Munuswami* AIR [1966] Mad 13

Consumer Protection Bill, 2015 such as the definition of 'Consumer' included the expression "buys and goods" and "hires or avails any services" include the transaction made through any modes including but not limited to offline electronic means of transaction, teleshopping or direct selling or multilevel marketing.[191] Furthermore, Section 32 enunciates the filing of complaint electronically and the payment of fees for such complaints in electronic form in order to save the time of the e-buyers.

1.8 MAJOR ISSUES AND CHALLENGES

- ***Capacity to contract***

In an e-contract, the essential ingredients must be complied with in order to make the contract valid. However, one major issue which needs to be dealt with is, whether the other party is a legally competent person to enter into a contract. The Service provider will have no idea whether the individual who has clicked on 'I Agree' or any similar icon is a competent person. As per Indian Contract act, 1872, it is one of the pre-requisites that only a legally competent person enters into a contract to make it a valid contract.[192] Contracts entered by individuals who are not competent to contract are void.

- ***Electronic Authentication***

In e-contracts, 'electronic records and digital signatures' constitute the medium for electronic authentication. Electronic records need to be validated under the rules of evidence and procedure. The Information Technology Act, 2000 stipulates for use of digital signatures to authenticate electronic records. The said Act accepts digital signature as a means of authentication[193] and provides a legal framework for facilitating and safeguarding electronic transactions. Section 3 of the act deals with the authentication of electronic records and provides that any subscriber may authenticate an electronic record by affixing his digital signature. The IT (Amendment) Act, 2008 inserted a new Section 3A pertaining to electronic signatures.[194]

[191] Section 2(8) Explanation (b) of the Consumer Protection Bill, 2015
[192] Section 11 of the Indian Contract Act, 1872
[193] Section 2(1) (p) of the Information Technology Act, 2000
[194] Jay and Briggs, "Information Technology and its Organizational Impact", Journal of Management Information Systems, Vol 13, No 3, Winter, 1997, p 4

- ***Choice of Law***

One of the major issues which need to be resolved in case of e-contracts is the law of jurisdiction which is referred to as 'Personal Jurisdiction' of the Court. Often the problem arising in a contract is with regard to the jurisdiction; when a party is a non-resident, which law would be applicable, i.e., domestic laws of the state where the party is residing or domestic laws of the state whose laws have been invoked in the offence being committed. In an online medium, fixing the choice of the law becomes a more complex issue compared to the normal contract.

1.9 LET'S SUM UP

In a nutshell, caution on the part of the consumer cannot be the only remedy for problems faced by e-consumer. Further,remedies available under the Indian Contract Act may not be feasible for easy solutions. E-consumerstherefore, require creative or at least easily accessible solutions in limited timespanfor daily dishonoured e-contracts.The Indian Legislature keeping in mind the end goal to control the rights andliabilities of gatherings if there should be an occurrence of Electronic Contracts has passed the ITAct, 2000 and the Electronic Commerce Act, 1998. The arrangements of these demonstrationsapprove the development of electronic contracts. The offer and acknowledgement given in type ofinformation messages will be held substantial. Anyway, the arrangements of the demonstrationare to be perused inconsistency with the Indian Contract Act, 1872 and the point and goals of theagreement ought not to be in negation to the arrangements of the Contract Act. We have likewiseobserved from different legal choices that offer, and acknowledgement given in the type of Emailswould be held as legitimate, and the agreement along these lines framed would tie. The ElectronicContracts are an amalgamated type of Cyber Law and Contractual law, and hence it gets itspower from both.

1.10 FURTHER READING

- Karnika Seth, Computers, Internet and New Technology Laws-A comprehensive reference work with special focus on developments in India. Lexis Nexis, Updated Edition 2013.

- NandanKamath, Law Relating to Computers Internet & E Commerce Universal Law Publisher, 5th Edition, (2012).
- AparnaViswanathan, Cyber Law Indian and International Perspectives, Lexis Nexis, 2012.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the additional requirements that need to be satisfied under E-Contract?

The following additional requirements are to be satisfied:

- Clear notice to the customer that the transaction is governed by the terms of a contract;
- An opportunity to review the terms of the standard form contract before agreeing to them; and
- A clear and unambiguous statement of what constitutes acceptance of the terms of the contract.

2. What are the requirements of 65B certificate?

A certificate issued is also admissible if it contains a statement which:

- Identifies the electronic record containing the statement.
- Gives information about the particulars of the computer involved in the production of the record.
- The certificate issued should be signed by a person officially responsible for the use of that device in relation to the relevant activity. The information fed into the computer should be in the appropriate form as well as by appropriate device.

3. What are the legal statues governing E-Contracts in India?

The legal statutes broadly addressing E-Contracts in India are the Indian Contract act, 1872, Information Technology Act, 2000, Indian Evidence Act, 1872.

1.12 ACTIVITY

Explain the evidentiary value of E-contracts with relevant cases along with the regulatory framework in other laws? (1000 words)

Unit 3:Comparative Analysis of E-Contract in Various Countries

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 India

1.4 United States of America

1.5 U.K.

1.6 Australia

1.7 Europe

1.8 Japan

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand:

- About the UNCITRAL Model Law
- The laws in India which govern the e-contracts
- Laws in other countries which regulate the use of e-contracts

1.2 INTRODUCTION

With the move towards modernization and reliance on the technological advancements, the lives of humans have become more sophisticated yet complex, and this aspect also applies to the

commercial transactions. In other words, it is undeniably the truth that electronic contracts, which serves as a means to acquire the goods and services in the modern times, encapsulates with itself great complexities.[195] One major contributor of the complexities is the popularity of the standard form of contracts, which also is increasing with time. On the other hand, the ways in which the people (consumers) acquire the goods and services have changed drastically, like today there is a massive market of e-commerce, and for a variety of reasons that is being given more importance and is continuously increasing in its valuation. However, in e-commerce, there are certain drawbacks as well which come handy, for instance, more often than not, the goods in these platforms are sold under the contract which contains clauses to exempt the liability of the seller, or to say the least, restrict it to very few conditions only. In such a situation, it would not be wrong to say that the concept of caveat emptor has taken a step back as there is no opportunity for the consumer to inspect the goods beforehand. In the light of the flaws that come implied with the e-contracts, it is very important that the laws are present to provide a proper safeguard to the consumers and to protect them from the unreasonable whims and fancies of the traders whose sole aim becomes to gain the profits by whatever means possible.[196]According to Sir William Anson a contract is legally binding agreement between two or more person where rights are acquired by one or more acts or forbearance on the part of the other E contract is an aid to drafting & negotiating successful contracts in e-commerce &related service. Following are some issues that are taken into consideration:

- European Directives
- U.K.-Electronic Communication Act
- Japan-The Law Concerning Electronic signature & certificate, 2000
- U.S.A.-Digital Signature Act 1995

In this chapter, we will be looking into these laws which govern the matter at hand, and will also compare them with those of other countries.

1.3 INDIA

In our day to day lives in the current lifestyle, the contracts have become so common, and their presence is so widespread that knowingly or unknowingly we enter into some of the other forms

[195] Ahmad, Tabrez (2009) Electronic Contracts: A Comparative Study of India and USA. India Law eJournal
[196]Sasso, Lorenzo (2016) Certain Comparative Noteson Electronic Contract Formation. Law. Journal of the Higher School of Economics 216-131

of the contracts everyday. In India, the law which deals with the contracts is the Indian Contract Act, 1872.[197] It lays down the requisites of a valid, enforceable contract, the communication regarding the essentials of the contracts, the manner in which they are to be executed, the breach of the contract, and the consequences of the breach of the contracts. It doesn't lay down the only manner in which the contracts are to be executed and other secondary things, and leaves adequate discretion with the contracting parties. In today's world, the internet has impacted almost every aspect of our lives, and the mode of entering into contracts hasn't been left untouched. With the internet, the world has indeed metaphorically become a smaller place as the modes of communication, among other things, have increased by courtesy of the technological development.[198] The importance of electronic contracts lies in the factors like requirement for speed, comfort and productivity. To substantiate this point, let's consider a hypothetical situation where a person 'X' from country 'A' wants to do some trade with person 'Y' from country 'B', for them to enter into a contract, there are basically 3 ways:-

a) The first one is that either X, or Y drafts 2 sets of agreement and sends it to the other person, and then the latter person signs the copies and then sends one of the copies to the first mentioned person.
b) The second one is that X and Y meet at some place and then sign the agreements, and then the contract gains its validity.
c) Now, in the third option, this entire transaction can take place in a couple of seconds, with the use of internet, as both X and Y can put their electronic signature in the electronic agreement and the electronic contract is formed, which to be very clear, has the same legal effect as any contract on paper.

The third option undoubtedly saves the delayed communications and the unnecessary monetary expenses.

In the initial phase, the countries were hesitant to accept this variety of contract and to make laws governing the same, but this was soon over and now countries have already put a law in place to acknowledge and regulate these types of contracts also. Needless to mention, that the laws which used to govern the traditional contracts couldn't be adequate to deals with the types of issues

[197] SV JogaRao, Computer Contracts & Information Technology Law (2nd Edition, 2005), pg. 182(Information Technology. Mathematical Markup Language (MathML) Version 3.0 2nd Edition)
[198] C.M. Abhilash, E Commerce laws in Developing countries: An Indian Perspective

thee-contracts brought with them. As far as India is concerned, the Indian Contract Act, 1872 wasn't equipped to deal with the technicalities of the e-contracts and thus the Information Technology Act, 2000 was enacted by the Parliament to deal with certain indispensable issues which came handy in the validity, development and execution of e-contracts.[199]

The Information Technology Act, 2000 recognizes and gives validity to the communications carried out by means of electronic data interchange. It also makes provisions for admissibility of electronic data as evidence in courts. Further, the courts have in the case laws have set precedents with the help of the legal provisions that the tape recordings, Compact Disks, email correspondences etc. are admissible and valid mode of evidence provided the proof is tendered in the manner laid down in the Indian Evidence Act. The Information Technology Act also provides for concepts like digital signatures as a mode of authentication, rules for determining electronic records.[200]

Traditional contracts as provided for by the Indian Contract Act 1872, are binding in nature and there are specific provisions which lay down the mode of the formation of contracts. But in respect of e-contracts, there is a lack of legal authorities to govern their formation and implementation. Further the recent instances raise a doubt on the security aspect.

It must have been understood by now that the problem which arises with e-contracts is the recognition and validity of the signatures of the parties which are in digital forms. So the laws which will be looked upto will be those dealing with the electronic signatures and not directly the e-contracts, as the validity and recognition to one implies and leads to that of the other one.

1.4 UNITED STATES OF AMERICA

The law on the use of electronic contract in the USA is the Digital Signature Act, 1995. USA became the first nation to pass a digital signature statute which intended to create assurance regarding the validity of the digital signature and thereby justify enforcement of obligations created by their use. Since then, many nations have passed similar legislation for governing the

[199]history.background - UNCITRAL Model Law on Electronic Contract <https://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/history.background.html>
[200]Kolekar, Yogesh Prasad. ―A Review of Information Technology Act, 2000 SSRN Electronic Journal, 2015

use of electronic signatures. The Digital Signature Act requires the use of certified asymmetric cryptosystem (public-key encryption) to verify the authenticity of the digital signature to be enforced. Therefore, to be enforceable and have legal validity, a digital signature must be issued with an intent to be enforced and also must utilize the required public-key encryption. The public key encryption must be certified by an authorized certification authority as under the laws of each state. Each state has to establish or authorize certifying authorities to issue certified digital signatures. However, their effect in the marketplace has been limited because of the encumbrance nature of the certification & encryption requirements.[201]

The UNCITRAL Model Law on Electronic Commerce was developed in response to the rapid changes that were taking place in the methods of communication used to conduct business and international trade.[202] As the use of electronic mail and electronic data interchange increased day by day and became more prevalent, the existence of legal impediments to electronic communications and uncertainty about their legal effect and validity became evident. The model law allows for the authentication of data by means of a signature. In America they provide that a document will be in a form acceptable to public authorities and courts. Therefore direction of Model Law on Electronic Commerce notes that for "all of the abovementioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met."[203]

The below discussed laws constitute the essential legal structure of electronic contracts in the United States:

The Uniform Electronic Transactions Act (UETA) is one among the several US Uniform Acts and an imperative U.S. enactment which is material to electronic contracts. UETA, as explicitly characterized in Articles 3 and 4, just applies to exchanges identified with business, business, and government matters; and to exchanges led by electronic means.

[201] Qin, Zheng Introduction to E-Commerce Springer Science & Business Media, 2010
[202]Rastogi, Sachin. Insights Into E-Contracts in India. 2014
[203]Florell, Dan. "Just A Click Away." National Association of School Psychologists.Communique, vol 43, no 4, National Association of School Psychologists, 1 Dec. 2014, p 36

The Electronic Signatures in Global and National Commerce Act (E-Sign Act), 2001: This Act perceives the legitimacy of agreements entered electronically, and where electronic marks have been used. The primary reason for the enactment of this Act was to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Uniform Computer Information Transaction Act (UCITA) is an important set of proposed guidelines relevant to the development of electronic contracts, particularly to those e-contracts on electronic materials, or computer data exchanges as the Act calls them. The member states of the USA were given the discretion to adopt or not to adopt the UCITA, and surprisingly UCITA has not been adopted by numerous states, and till date only 2 of the states (Maryland and Virginia) did adopt it, and 4 other states passed anti-UCITA laws.

1.5 U.K.

The use of e-contracts in U.K. is governed by the Electronic Communication Act, 2000. The first draft of a bill, the Electronic Communication Bill was published in July 1999 although it was withdrawn when it attracted a great deal of attention regarding key escrow & provisions that were later incorporated into the Regulation of Investigatory Powers Act 2000.The Act received the royal assent on May 26, 2000.

Electronic Signature in the U.K.- The Act provides a definition in Section 7(2)- The term authentication has two meaning in the content of Information Security. In the U.K. an electronic signature is admissible under the provisions of Section 7(1)(a).The authenticity of data can be admissible where any person certifies the signature. The certificate would normally be provided by an entity such as a trusted third party. Although it does not follow that such a certificate has to be provided by a trusted third party.[204]

1.6 AUSTRALIA

[204]Electronic Signatures in Law on JSTOR
<https://www.jstor.org/stable/j.ctv5137w8>

In Australia, Electronic Transaction Act, 1999 the corresponding state and territory legislation is not comprehensive code of rules, nor does it govern all aspects of electronic contracting or of e-commerce's essential procedure and principles, intended to promote global regulating harmony in relation to electronic transactions.[205] The two basic principles underlying the Australian Electronic Transactions Act are functional equivalence (i.e. that paper-based commerce and electronic commerce are to be treated with equality) and technology neutrality. In accordance with the UNCITRAL Model Law on this matter, the Australian Electronic Transaction Act does not involve heavy regulations to promote the validity of transactions involving electronic commerce. Further, Australia has publically declared their intention to adopt the UN Convention on the Use of Electronic Communications in International Contracts but hasn't acted upon it yet, and for complying with the obligation under the mentioned convention, it will need to update the Electronic Transaction Act.[206]

1.7 EUROPE

For the validity of e-contracts, the validity of e-signature is of prime concern. The Electronic Signature Directive (1999/93/EC) was a European Union Directive on the use of e-signatures in e-contracts which has now been replaced by Electronic Identification, Authentication and Trust Services(eIDAS)(Regulation 910/2014). The basic and most important directive of 1993 Directives, is mentioned under Article 5, which provides that electronic signatures must be recognized and given equal standing and effect in law as that is attributed to written signatures.[207]

Conclusion of online contracts in Europe- the Directives address the fundamental requirements to determine when a contract is concluded electronically. The mechanism of concluding a contract specified in the Articles of the Directives goes further than required by the traditional concept of offer and acceptance by adding the requirement that the recipient receives electronically the provider acknowledgement of acceptance. The objective of the Directive is to reduce obstacles and to ensure that the differences concerning the legal recognition of electronic signature do not become restrictions on the free movement of products between the member

[205]Alghamdi, Abdulhadi M. The Law of E-Commerce: E-Contracts, E-Business. AuthorHouse, 2011
[206]Dr.Lakshmi T and Rajeshkumar S "In Vitro Evaluation of Anticariogenic Activity of Acacia Catechu against Selected Microbes" IRJMST, March 2018
[207]Harlow, Carol, and Richard Rawlings.—Contract, Contract, Contract Law and Administration, pp 393–436

states by creating a harmonized legal framework for the use of electronic signature within the EU and establishing a set of rules which form the foundation for legal recognition of electronic signatures.

The eIDAS which have replaced the previous Directives have come in effect from 1st July, 2016, and it sets out rules for electronic identification and trust services. These services help verify the identity of individuals and businesses online or the authenticity of electronic documents.

1.8 JAPAN

The law in the country of Japan governing the matter in hand is the Electronic Signature & Certification Service (Law No. 102 of 2000), which has been in force since April1 2001.[208] According to Article 3 of supplementary provisions, the government is required to examine how the law has been enforced & to undertake revisions where necessary. The law defines an electronic signature as measures are as follow:-

- Measures to indicate that the information was created by the person who performed
- Measures that can confirm whether or not any alteration of the information has been performed.

This definition requires the need to identify the person signing the data & for the ability to confirm whether the data has been altered since it was signed. In essence, this definition only provides for a digital signature & thereby precludes the use of other forms of electronic signature. Article 3 provides for the presumption that data is authentic, where the electronic signature is performed by the principles.[209]

1.9 LET'S SUM UP

In this chapter, we discussed how e-contracts has been put to use in different countries and how different countries have regularized e-contracts. Finally, we ended the discussion with a comparative analysis of the laws in India, USA, UK, Australia, Europe and Japan.

1.10 FURTHER READING

[208]Weakley, Suzanne L California Law of Contracts: 2017 Update CEB, 2017

[209]Trishala A , Lakshmi T and Rajeshkumar S,— Physicochemical profile of Acacia catechu bark extract –An In vitro study" IRJMST, April 2018

- Alghamdi, Abdulhadi M. The Law of E-Commerce: E-Contracts, E-Business. AuthorHouse, 2011.
- Barnett, Randy E. ―Contract Is Not Promise; Contract Is Consent.‖ Philosophical Foundations of Contract Law, 2014, pp. 42–57.
- Hedley, Steve. The Law of Electronic Commerce and the Internet in the UK and Ireland. Taylor & Francis, 2017.
- Reed, Kathleen, et al. Contract Law for Paralegals: Traditional and E-Contracts. Pearson Higher Ed, 2012.
- Tepper, Pamela. The Law of Contracts and the Uniform Commercial Code. Cengage Learning, 2014.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Which provisions of the IT Act, 2000 governs the manner of producing electronic records as evidence in a court of law?**

   None. The Indian Evidence Act deals with the concerned situation.

2. **Does the Uniform Computer Information Transaction Act (UCITA) apply to every member state of the USA?**

   No. Only 2 states have ratified the UCITA.

3. **Name the states which have ratified UCITA.**

   Maryland and Virginia

4. **Which law governs the e-contracts in Australia?**

   Electronic Transaction Act, 1999

5. **Which law governs the e-signatures in Europe?**

   The Electronic Signature Directive (1999/93/EC) was a European Union Directive on the use of e-signatures in e-contracts which has now been replaced by Electronic Identification, Authentication and Trust Services(eIDAS)(Regulation 910/2014)

1.12 ACTIVITY

Find out whether India is a signatory to the UN Convention on the Use of Electronic Communications in International Contracts? Find about all the signatories of the convention and whether their laws comply with the guidelines set in the Convention. (1000 - 1500 words)

Unit 4: Exercise of Jurisdiction and Issues Related Therewith

4

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Jurisdictions over Internet Transactions
1.4 Multiple Jurisdiction and their applicability
1.5 Governing law
1.6 Conclusion
1.7 Let's sum up
1.8 Further reading
1.9 Check your progress: Possible answers
1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand

- Issues of Jurisdiction Related to E-Contracts
- Barriers in E-Commerce vis-à-vis jurisdiction
- Jurisdiction of Courts Under E-Contracts

1.2 INTRODUCTION

The presence of internet and netizensare ubiquitous in today's times. Internet is international and allows access to people from almost every corner of the world. Most websites do not even contain the geographical address that aid in detecting the jurisdiction of the activities associated

with such websites.[210] Effectively, parties involved in transactions taking place in cyberspace are not concerned with the geographical location of the site through which the transaction is made. The manner in which the internet has dissolved all physical boundaries has given rise to the issue of jurisdiction, which in turn becomes relevant in instances where disputes arise relating to such transactions conducted online.

'Jurisdiction' effectively means the judicial, legislative, administrative compliances that the states enjoy over the respective territories that they own and control. For disputes that arise offline, traditional processes as followed in courts through the litigation system are used to dissolve them, which involve remedies that are primarily structured as per the territories concerned and the local and national laws. However, since the internet is indifferent towards all forms of locational constraints, traditional jurisdictional laws do not hold much significance over such activities. However, in the event the parties involved in a dispute arising overuse and exploitation of cyberspace belong to the same territory, the territorial jurisdictional laws can be implemented in the same manner that they apply to offline disputes. But instances wherein parties belong to different jurisdictions give rise to complications of various kinds. The importance of jurisdiction lies in the fact that parties involved in a potential dispute need to be able to predict the magnitude of their liabilities relevant to the specific jurisdiction concerned, and consider the legal and practical expenses associated with defending the dispute in such specific jurisdictions. The factors to be taken into consideration during the determination of jurisdiction are as follows:[211]

- The location where the parties are based
- The location where the commercial activity has taken place
- Factors connecting the parties to one another
- Application of private international law rules vis-à-vis the dispute concerned

1.3 JURISDICTION OVER INTERNET TRANSACTIONS

[210] VivekSood, "Cyber Law Simplified" (2001), p 186, Tata Mcgraw Hill Publishing Co Ltd, New Delhi

[211] S.K. Verma and Raman Mittal, "Legal Dimensions of Cyber Space", (2004), Indian Law Institute, New Delhi at p 266

As per traditional practices, there are two factors that play a significant role in determining the jurisdiction associated with dispute concerned; one, the place where the defendant resides; and two, the place where the cause of action arises.[212] However, owing to the extra-territorial nature of the internet in general, the application of either of the aforementioned factors becomes very challenging. For example, if an individual residing in India wishes to pay and download an article from a website, and makes the payment online through a debit or a credit card but is thereafter unable to perform the download, he might want to sue the owner of the site for the dispute arising. In the event the owner is a resident of Thailand, there arises a jurisdictional issue, which becomes further complicated if the website itself is based in the server in Brazil.

Such jurisdictional issues arising in association with e-contracts have, to an extent, been addressed under the Information Technology Act, 2000. Section 13 of the IT Act[213] mentions the manner of determining the time and place of dispatch and receipt of electronic records and addresses concerns related to the issue of deemed jurisdiction in electronic contracts by stating that

"(1) … Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator. (2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(i) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

[212] Adrian Briggs, "The Conflict of Laws", Claredon, Oxford, 2002
[213] Section 13: Time and place of dispatch and receipt
<https://www.itlaw.in/section-13-time-and-place-of-despatch-and-receipt-of-electronic-record/>

(b) if the addressee has not designated computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee; an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section:

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered."

In the case of ***PR Transport Agency Vs. Union of India***[214], the Allahabad High Court addressed the issue of jurisdiction in an instance wherein the respondent had sent a letter of acceptance through email to the petitioner's email address, but had subsequently sent another email cancelling the auction in favour of the petitioner owing to 'technical and unavoidable reasons'. After the petitioner challenged the communication before the Allahabad High Court, the respondent raised objections relating to the territorial jurisdiction of the court on grounds that the no part of the cause of action had arisen in Uttar Pradesh, which is to imply that the Allahabad High Court shall have no jurisdiction to try the dispute. The principal place of business of the petitioner in the case was in Chandauli, Uttar Pradesh, and hence, the court applied section 13(3) of the IT Act, 2000, and held that the acceptance of the tender by email would be considered deemed received by the petitioner at Chandauli, i.e., the place of the petitioner's business, and

[214] *PR Transport Agency v Union of India* AIR [2006] All 23

hence the Allahabad High Court shall have jurisdiction to try the dispute.

Therefore, in view of the foregoing, it could be stated that the determination of the place of contract in an e-contract for the purposes of resolving disputes relating to jurisdiction would be deemed to be the place where the originator has his/her place of business and where the addressee has the place of business. However, with regards to the fact that section 13 of the IT Act, 2000 is subject to the mutual agreement of the contracting parties, it is always convenient that the parties always include a specific clause on the jurisdiction in their agreements.[215]

1.4 MULTIPLE JURISDICTION AND THEIR APPLICABILITY

Transactions conducted over the internet often involve parties who are located in different countries across the world which have their own and individual legal systems, which might lead to ambiguities regarding the place of the disputed activities, especially in instances wherein the technology systems and computer servers are located in different regions. It is in instances like these that the scope and application of private international laws and their principles become relevant.[216]

Principles of private international law aim at resolving issues that arise out of foreign components in legal relationships. From a global perspective, it is understood that private international law principles resolve issues related to jurisdiction and application of the law regarding enforcement of foreign judgments. From a general perspective as well, principles of private international law form a part of municipal law that aims to regulate the conduct between two private parties, which in turn assumes an international character because of the foreign element existing in the legal relationship. Given the international nature of cyberspace and the potential scope of the parties involved in such transactions being associated with multiple countries to the extent of giving every court possible in every country related a jurisdiction over

[215]The Electronic Transactions Act 2010 <https://www.lexology.com/library/detail.aspx?g=5e20c761-4ccd-4de3-8c0d-5c6eb6a9f2e1>

[216]Mapping Employee Experience Stages to Your Technology <https://www.cmswire.com/digital-workplace/mapping-employee-experience-stages-to-your-technology-landscape/>

an occurring dispute,[217] principles of private international law become useful for they inter alia address contexts such as:

- Jurisdiction to adjudicate a dispute at a specific location (i.e., the forum concerned, and/or the situs)
- The law applicable to the dispute concerned
- Enforceability of preceding judgments in courts of foreign jurisdictions

1.5 GOVERNING LAW

Under traditional contracts, the governing law that applies is generally seen to be the laws of the state wherein the transaction takes place, unless, the parties to the contract agree otherwise and include the same in the agreement vide a clause. In the case of the latter, principles of private international law apply, especially in the case of transnational contracts. However, e-contracts might involve having parties belonging to different countries, giving away no specific factor to determine the place of the consummation of the contract. As a result, courts in motion often tend to apply the law of the country that has the closest and the most substantial connection with the contract. Nevertheless, various courts take various factors into consideration for establishing such a connection with the e-contract concerned.

E-contracts, hence, specify both the jurisdiction and the governing law applicable in case of resolving disputes arising and accruing out of an e-contract. In such instances, the court upholds party autonomy and gives precedence to the terms of the contract. However, in case of B2C contracts, exceptions are carved out to address instances that involve forum shopping by the party in authority owing to the unequal bargaining power of consumers in determining the jurisdiction and governing law in such transactions.[218] Various jurisdictions have included provisions of law in their domestic legal frameworks with a view to addressing this; for example, section 28 of the Indian Contract Act, 1872 states that[219]

[217] Wolters Kluwer Portal "Computabel contracts/E-contracting" (2014) <https://goo.gl/5YAtBq>
[218] Mindy Chen-Wishart, Formation and Third Party Beneficiaries (Oxford University Press 2018) 72
[219] Void Agreements - KLE Society's Law College

"Every agreement, -

(a) by which any party thereto is restricted absolutely from enforcing his rights under or in respect of any contract, by the usual legal proceedings in the ordinary tribunals, or which limits the time within which he may thus enforce his rights; or (b) which extinguishes the rights of any party thereto, or discharges any party thereto from any liability, under or in respect of any contract on the expiry of a specified period so as to restrict any party from enforcing his rights, is void to that extent.

Exception l.-This section shall not render illegal a contract, by which two or more persons agree that any dispute which may arise between them in respect of any subject or class of subjects shall be referred to arbitration and that only the amount awarded in such arbitration shall be recoverable in respect of the dispute so referred.

Exception 2. Nor shall this section render, illegal any contract in writing, by which two or more persons agree to refer to arbitration any question between them which has already arisen, or affect any provision of any law in force for the time being as to references to arbitration."

This, in turn, means that the laws of our country provide to its consumer's protection by way of allowing the court leeway to disregard the agreement between the consumer and the seller in so far as the choice of forum and the governing law are concerned.[220]

1.6 CONCLUSION

Notwithstanding the varying approach across jurisdictions laying down specific laws related to jurisdictions, and the global nature of cyberspace which creates complications with respect to determination of jurisdiction for the purposes of resolving disputes arising in connection with execution and implementation of e-contracts, the general and common intention of the respective legislature, as well as judiciary of almost all the states, addresses that acts or omissions performed shall continue to be as valid if performed electronically and/or digitally as they would be had they been performed traditionally, as long as they are legally acknowledged and

<http://www.klelawcollege.org/kle/wp-content/uploads/2017/10/9.Void-Agreements.pdf>

[220]Alexandra Bleoanca, "Earlier stage in the electronic contract conclusion" [2010] ISSN 1220-8512

approved, and contains all the attributes of a legally valid contract in accordance with the applicable laws. [221]

However, notwithstanding the foregoing, it cannot be denied that determination of territorial jurisdiction in case of e-contracts becomes especially complicated in instances wherein no geographical and/or national boundaries have been laid down either by the existing laws or in exercise of party autonomy through the contract, to address the execution and implementation of such contracts, in part of in full. Admittedly, the IT Act, 2000 and general judicial interpretations related to contracts clarify the jurisdictional aspects of e-contracts to a certain extent; nevertheless, it is easier and more convenient to address disputes arising in relation to e-contracts if the parties therein have mutually agreed upon and specified both the jurisdictional aspects and the provisions on governing law in the concerned e-contract, so as to avoid future conflicts on issues regarding jurisdiction or choice of law.

As would be evident from this chapter, there is currently an unmistakable scarcity of one uniform international legal instrument and/or international laws in general that shall apply equally and universally to all territories comprehensively to govern all electronic contracts within their ambits. The introduction of such an act would aid and assist in ensuring and establishing a uniform and enhanced level of consumer protection, would promote a reduction in transactional costs incurred by entrepreneurs, would accelerate and simplify procedures required to be undergone for the purposes of settlement of disputes arising in connection with electronic contracts. Furthermore, the continuous development in the world of technology today demands development as well as persistent upgradation and development of the legal systems and frameworks associated with the functioning and regulation thereof, so as to ensure fair distribution of rights and responsibilities amongst the parties involved.

1.7 LET'S SUM UP

In this chapter, we studied the jurisdictional aspects in electronic contracts and how jurisdiction works over Internet Transactions. We also discussed the multiple jurisdictions and their

[221] Adam J Mambi, ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community (African Books Collective, 2010) 47

applicability and finally ended the discussion with the governing law with respect to it.

1.8 FURTHER READING

- S.K. Verma and Raman Mittal, "Legal Dimensions of Cyber Space", (2004), Indian Law Institute, New Delhi at p. 266.
- VivekSood, "Cyber Law Simplified" (2001), p. 186, Tata Mcgraw Hill Publishing Co. Ltd., New Delhi.
- J. E. Hill, The Future of Electronic Contracts in International Sales: Gaps and Natural Remedies under the United Nations Convention on Contracts for the International Sale of Goods, 2 Nw. J. Tech. &Intell. Prop. 1 (2003), p. 5.
- G. Ruhl, Party Autonomy in the Private International Law of Contracts: Transatlantic Convergence and EconomicEfficiency. CLPE Research Paper No. 4/2007; Conflict of Laws in a Globalized World, Eckart Gottschalk, RalfMichaels, GieselaRühl& Jan von Hein, eds., Cambridge University Press, p. 4.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of jurisdiction under e-contracts?

'Jurisdiction' effectively means the judicial, legislative, administrative compliances that the states enjoy over the respective territories that they own and control. For disputes that arise offline, traditional processes as followed in courts through the litigation system are used to dissolve them, which involve remedies that are primarily structured as per the territories concerned and the local and national laws.

2) What are the factors that need to be taken into consideration while determining jurisdiction?

The factors to be taken into consideration during the determination of jurisdiction are as follows:

- The location where the parties are based
- The location where the commercial activity has taken place

- Factors connecting the parties to one another
- Application of private international law rules vis-à-vis the dispute concerned

3) What are the traditional practices that take place over internet transactions?

As per traditional practices, there are two factors that play a significant role in determining the jurisdiction associated with dispute concerned; one, the place where the defendant resides; and two, the place where the cause of action arises.

4) What does Private international law address with respect to e-contracts?

- Jurisdiction to adjudicate a dispute at a specific location (i.e., the forum concerned, and/or the situs)
- The law applicable to the dispute concerned
- Enforceability of preceding judgments in courts of foreign jurisdictions

1.10 ACTIVITY

Explain the jurisdictional issues and challenges pertaining to internet transactions and e-contracts with relevant provisions and case laws? (1000 words)

Block 4

International Perspective

Unit 1: Importance of International Organization in E-Commerce

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 E-Commerce: A Global Analysis

1.3 Who sets the rules for E-commerce?

1.4 Who addresses E-commerce at the national level?

1.5 Importance of NGOs in E-commerce law and policy development process

1.6 International Organizations involved in E-commerce law

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The International perspective of e-commerce
- Who sets the rules for e-commerce
- Importance of NGOs in E-commerce

1.2 E-COMMERCE: A GLOBAL ANALYSIS

The most important elements of e-commerce law relate to the fundamental components of commercial transactions – how to ensure that an online contract is as valid and enforceable as one consummated offline. The building blocks of e-commerce law, therefore, focus on both

enforcing the validity of electronic contracts and ensuring that the parties can be held to their bargains.[222]

Once the contractual issues have been addressed, e-commerce law analysis shifts to a series of legal issues that may govern the transaction. These include jurisdiction (which court or arbitral tribunal can adjudicate a case), consumer protection issues, taxation, privacy, domain name disputes, as well as the role and potential liability of intermediaries such as Internet service providers.

1.3 WHO SETS THE RULES FOR E-COMMERCE?

Several organizations contribute to the development of global e-commerce law at the international level. Different organizations have tended to take the lead on different issues:[223]

- UNCITRAL has played a leading role in developing model laws for e-commerce transactions;
- OECD has been at the forefront of Internet taxation, e-commerce consumer protection and privacy;
- WIPO has been the international leader on digital copyright and trademark issues involving domain names;
- ICANN has implemented the Uniform Domain Name Dispute Resolution Policy, which has addressed thousands of domain name disputes;
- APEC has worked on digital divide concerns and small and medium-sized enterprise (SME) e-commerce adoption;
- The Hague Conference on Private International Law has been the worldwide leader on Internet jurisdiction issues;
- WTO has considered e-commerce trade barriers.

[222] Nair, Kiran (2017) Impact of E-Commerce on Global Business and Opportunities - A Conceptual Study. International Journal of Industrial Engineering and Management Research. 2 324-336

[223]Panagariya, A E-Commerce, WTO, and Developing Countries. *Policy issues in international trade and commodities study Series* No.2 UN, New York and Geneva. 2000, pp 1-33

1.4 WHO ADDRESSES E-COMMERCE AT THE NATIONAL LEVEL?

E-commerce law frameworks at the national level vary by country. In some countries, such as Japan, India, Malaysia, South Africa and Columbia, most of the e-commerce law and policy initiatives come from the national government. The United States and Canada use a dual approach whereby both the federal and state/provincial governments play a role, while in the European Union, directives applicable in all Member States are often the most important source of legal guidance.[224]

1.5 IMPORTANCE OF NGOs IN E-COMMERCE LAW AND POLICY DEVELOPMENT PROCESS

On certain issues, such as jurisdictional rules and consumer protection, NGOs play a critical role in the development of e-commerce law and policy as they are often accorded a place at the negotiating and drafting table.[225] At other times, the role of the NGO is more reactive, responding to new proposals and lobbying on behalf of the business or consumer interests.

1.6 INTERNATIONAL ORGANIZATIONS INVOLVED IN E-COMMERCE LAW

a) UNCITRAL

UNCITRAL is the United Nations Commission on International Trade Law. Established by the United Nations in 1966 to harmonize the law of international trade, it is a core legal body of the United Nations system that works to create accessible, predictable and unified commercial laws.

The Commission is composed of 36 Member States elected by the General Assembly, are chosen to represent the world's various geographic regions and its principle economic and legal systems.

[224]Malkawi, B H E-commerce in Light of International Trade Agreements: The WTO and the United States-Jordan Free Trade Agreement. *International Journal of Law and Information Technology*, Vol. 15 No.2, 2007, 153-169

[225] ECLAC *Electronic Commerce, International Trade and Employment: Review of The Issues*. UN, Economic comission for Latin America and the Caribbean ECLAS, Washington Office, April 2002, pp 1-30

Members are elected for terms of six years, with the terms of half the members expiring every three years. The UNCITRAL Secretariat is located in Vienna and carries out its work in annual sessions, which are held in alternate years in New York and Vienna. All States and interested international organizations are invited to attend as observers and participate in sessions of the Commission and of its working groups.[226]

UNCITRAL focuses on law reform and creating model commercial laws that are both accessible and predictable. This is accomplished through:

- Conventions, model laws and rules which are acceptable worldwide
- Legal and legislative guides and practical recommendations
- Updated information on case law and enactments of uniform commercial law
- Technical assistance in law reform projects
- Regional and national seminars on uniform commercial law.

The Commission has established six working groups to perform the substantive preparatory work on a range of topics, including the international sale of goods; international transport of goods; international commercial arbitration; public procurement and infrastructure development; construction contracts; international payments; cross-border insolvency and, most important for current purposes, electronic commerce.

WHAT IS UNCITRAL'S INVOLVEMENT WITH E-COMMERCE?

UNCITRAL created a Model Law on Electronic Commerce in 1996 to enhance the use of paperless communication. In 2001, it created a Model Law on Electronic Signatures. Future electronic commerce work will focus on: electronic contracting, with a view to creating a draft convention; online dispute settlement;[227] dematerialization of documents of title; and a convention to remove legal barriers to the development of electronic commerce in international trade instruments.[228]

[226]WTO. Study from WTO Secretariat highlights potential trade gains from electronic commerce, available at <http://www.wto.org/english/newse/pres98e/pr96e.htm>
[227] UNCITRAL, Model Law on International Credit Transfers, UN, 1992
[228]Ham, S and Atkinson, D R a third way framework for global e-commerce. Progressive Policy Institute, Technology & New Economy Project, March, 2001, 1-29

b) OECD

The Organisation for Economic Co-operation and Development (OECD) grew out of the Organisation for European Economic Cooperation, which administered American and Canadian aid to Europe after World War II. Established in 1961, OECD today has 30 member countries and maintains active relationships with 70 more. Its goals are to build strong economies in its member countries, improve market systems, expand free trade and contribute to development in both industrialized and developing countries. The governing body of OECD, the Council, is led by a secretary-general and is made up of representatives of member countries, who provide guidance on the work of OECD committees and decide on the annual budget.[229]

OECD facilitates the creation of international instruments, decisions and recommendations in areas where multilateral agreements may create progress for individual countries in a globalized economy. Its various directorates and committees analyse issues, identify policies and deal with a wide range of economic and social issues from macroeconomics to trade, education, development and science and innovation. Among its other functions, OECD:[230]

- has published more than 4 000 publications including research reports, conventions, working papers, country surveys and statistics spanning the spectrum of socio-economics;
- promotes and develops international statistical standards and coordinates statistical activities with other international agencies;
- fosters good governance in the government and private sectors through the hosting of conferences and the development of policy and guidelines;
- identifies and analyses issues surrounding emerging economies, sustainable development and aid.

WHAT IS OECD'S INVOLVEMENT WITH E-COMMERCE?

E-commerce has become an area of focus for OECD because of its trans-border nature and its potential for all countries in the areas of economic growth, trade and improved social conditions. It has developed policy in areas ranging from telecommunication infrastructure and services to

[229]Oliner, S.D., and Sichel, D.E. The Resurgence of Growth in the Late 1990's: Is Information Technology the Story? Journal of Economic Perspectives, Volume 14, Number 4, Fall.2000

[230] OECD E-commerce: Impacts and Policy Challenges. Economic Outlook 67, 2000

taxation, consumer protection, network security, privacy and data protection, as well as emerging markets and developing economies.[231]

Following its "OECD Action Plan for Electronic Commerce", endorsed by its members in 1998, its work programme focus is to build trust for users and consumers; establish ground rules for the digital marketplace; enhance the information infrastructure for e-commerce; and maximize the benefits of e-commerce. Some of the activities currently underway in the area of e-commerce include:

- implementing aspects of the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce;
- promoting the use of privacy-enhancing technologies and user education and awareness about online privacy issues;
- studying the effects of e-commerce on cross-border trade in financial services, on contract law and electronic delivery of insurance products;
- studying access to high-bandwidth information and communication technologies at affordable costs in rural as well as in urban areas;
- researching the needs for and constraints to, capacity development for trade faced by developing countries; and
- disseminating its work on e-commerce to member and non-member countries through other international organizations.

c) <u>WIPO</u>

The World Intellectual Property Organization (WIPO) is an international organization that promotes and protects original works in the realms of art, science and technology.

Headquartered in Switzerland, WIPO is one of the 16 specialized agencies of the United Nations. It administers 23 international treaties dealing with different aspects of intellectual property protection (both industrial protection and copyright) and has more than 170 Member States.

[231]OECD ICT Key Indicators.Information Technology Outlook. 2010. [35] IMF, World Economic Outlook, 2006/2011

Although WIPO was formed in 1970, its roots go back as far as the 1883 Paris Convention for the Protection of Industrial Property. In 1974, WIPO became a specialized agency of the United Nations with the mandate to administer intellectual property matters recognized by the Member States of the United Nations.

WIPO's main objective is to develop international standards for the protection of intellectual property in keeping with ongoing advances in technology and business. Through its treaties, it seeks to:

- harmonize national intellectual property legislation and procedures;
- provide services for international applications for industrial property rights;
- exchange intellectual property information;
- provide legal and technical assistance to developing and other countries;
- facilitate the resolution of private intellectual property disputes; and
- marshal information technology as a tool for storing, accessing and using valuable intellectual property information.

WHAT IS WIPO'S INVOLVEMENT WITH E-COMMERCE?

WIPO has created a Digital Agenda to respond to the confluence of the Internet, digital technologies and the intellectual property system. Through international discussions and negotiations, WIPO is formulating new ways in which intellectual works can be disseminated, while at the same time ensuring the rights of their creators remain protected.

The Digital Agenda also aims to:

- integrate developing countries into the Internet environment through such tools as the use of WIPOnet and the electronic delivery of information and services;
- rethink how intellectual property law works in Internet transactions and examine emerging new norms in this respect;
- facilitate the creation of effective online systems to resolve disputes; and

- Coordinate and ensure the development of efficient and consistent responses to common concerns across national and multi-sectoral boundaries.

d) ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is a technical coordination body for the Internet. Created in October 1998 by a broad coalition of the Internet's business, technical, academic and user communities, ICANN has assumed responsibility for a set of technical functions previously performed under United States Government contract by other groups.[232]

As a non-profit, private-sector corporation, ICANN is dedicated: to preserving the operational stability of the Internet; to promoting competition; to achieving a broad representation of global Internet communities; and to developing policy through private-sector, bottom-up, consensus-based means. ICANN welcomes the participation of any interested Internet user, business or organization. The Board of ICANN has currently composed of nineteen directors: nine at-large directors, nine selected by ICANN's three supporting organizations and the president/CEO (*ex officio*). Five of the current at-large directors were selected by an Internet users' vote.

ICANN coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:

- Internet domain names
- IP address numbers
- protocol parameter and port numbers.

In addition, ICANN coordinates the stable operation of the Internet's root server system.

WHAT IS ICANN'S INVOLVEMENT WITH E-COMMERCE?

Future ICANN work is likely to address several key issues including institutional reform, the participation of Internet users in the policy-making process, the establishment of new top-level domains and amendments to ICANN's domain name dispute resolution process.

[232] Huang Lijin, The economic impact of the network on international trade. Foreign trade: economy, international trade, 2010

e) THE HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW

The Hague Conference is an intergovernmental organization that works to unify private international law rules. The first session of the Hague Conference was held in 1893; after seven more sessions, a statute came into force in 1955, making the Conference a permanent organization.

The Conference, which has 59 Member States, holds plenary sessions every four years to discuss and adopt draft conventions and recommendations and make decisions on the working agenda of the Conference. Non-Member States invited to participate on an equal footing with Member States can vote at plenary sessions. The Conference is organized by a secretariat (the Permanent Bureau) which has its seat at The Hague and whose officials must be of different nationalities. The Bureau organizes the plenary sessions and maintains contacts with the Member States, international organizations and users of the conventions.[233]

The principal role of the Conference is to negotiate and draft multilateral treaties (conventions) in the different fields of private international law (e.g. international judicial and administrative cooperation; conflict of laws for contracts, torts, maintenance obligations, status and protection of children, relations between spouses, wills and estates or trusts; jurisdiction and enforcement of foreign judgments). Currently, its areas of concern include:

- conflict of jurisdictions;
- applicable law and international judicial and administrative cooperation regarding civil liability for environmental damage;
- problems of private international law raised by electronic interchange; and
- maintenance (support) obligations.

WHAT IS THE HAGUE CONFERENCE'S INVOLVEMENT WITH E-COMMERCE?

In 1999, the Conference held a round-table discussion (in conjunction with the University of Geneva) with experts in various fields on issues arising from e-commerce and Internet

[233] Sun Liyun, YanchunRong, International e-commerce and conventional international trade. Ppractices of international trade, 2011

transactions. A series of recommendations were adopted in such areas as online contracts, business-to-business and business-to-consumer transactions and online dispute resolution.ṅ[234] In June 2001 the Conference held its Nineteenth Session to work towards a new Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters and to decide on its future work programme. Delegates based their discussions on both a Preliminary Draft Convention drawn up in October 1999 and on the results of formal and informal meetings of experts on e-commerce and intellectual property.

f) WTO

The World Trade Organization (WTO) is an international organization that deals with the rules of trade between nations. Based in Switzerland, WTO was formed in 1995 as the successor of the General Agreement on Tariffs and Trade (GATT), which set up a multilateral trading system shortly after World War II. Today WTO has over 130 member nations, more than 75% of which are developing or least-developed countries.[235]

A series of rounds of trade negotiations under GATT and WTO have led to agreements between governments on various aspects of the trade, tariffs, telecommunications and financial services. These agreements help set the ground rules for international trade and commerce. Decisions are made by the entire membership, generally by consensus. WTO hosts a ministerial conference that generally meets every two years. Several other levels of councils and committees work on a wide variety of issues.

The primary functions of WTO are to:

- administer WTO trade agreements;
- act as a forum for trade negotiations;
- handle trade disputes;
- monitor national trade policies;
- provide technical assistance and training for developing countries; and

[234]INTERNATIONAL TELECOMMUNICATION UNION <https://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc>

[235] Kraemer, K L J Gibbs and JDedrick Impact of globalization on ecommerce adoption and firm performance: a cross- country investigation. Mimeo, Irvine, CA.2002

- work together with other international organizations.

WHAT IS WTO'S INVOLVEMENT WITH E-COMMERCE?

At the 1998 ministerial meeting, WTO members agreed to study trade issues arising from global electronic commerce, focusing on three questions:

- how do existing WTO agreements impact e-commerce?
- are there any weaknesses or omissions in the law which need to be remedied?
- are there any new issues not now covered by the WTO system on which members want to negotiate new disciplines?

Since then, issues related to e-commerce have been examined by WTO councils in the areas of services, goods, intellectual property and trade and development. A seminar on "Government Facilitation of E-commerce for Development" was held in June 2000, at which speakers from developing and developed countries, international organizations and the private sector addressed issues related to e-commerce and development. Each of WTO bodies working on e-commerce issues has produced progress reports for the General Council.

1.7 LET'S SUM UP

In this chapter, we have studied the global analysis of E-Commerce along with who sets the rules for E-Commerce and who addresses E-Commerce at the national level. We also studied the importance of NGOs and finally, we ended the discussion with International organizations involved in E-Commerce.

1.8 FURTHER READING

- Shahriari, Shahrzad&Shahriari, Mohammadreza&gheiji, Saeid. (2015). E-COMMERCE AND IT IMPACTS ON GLOBAL TREND AND MARKET. International Journal of Research - GRANTHAALAYAH. 3. 49-55.
- Reynolds, Jonathan. (2000). E-commerce: A critical review. International Journal of Retail & Distribution Management. 28. 417-444. 10.1108/09590550010349253.
- Smith, Katherine. (2008). An Analysis of E-Commerce: E-Risk, Global Trade, and Cybercrime. SSRN Electronic Journal. 10.2139/ssrn.1315423.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) Who sets the rules for E-commerce?

Different organizations have tended to take the lead on different issues:

- UNCITRAL
- OECD
- WIPO
- ICANN
- APEC
- The Hague Conference on Private International Law
- WTO

2) Who addresses E-commerce at the national level?

E-commerce law frameworks at the national level vary by country. In some countries, such as Japan, India, Malaysia, South Africa and Columbia, most of the e-commerce law and policy initiatives come from the national government. The United States and Canada use a dual approach whereby both the federal and state/provincial governments play a role, while in the European Union, directives applicable in all Member States are often the most important source of legal guidance.

3) What the objective of digital agenda under WIPO?

- integrate developing countries into the Internet environment through such tools as the use of WIPOnet and the electronic delivery of information and services;
- rethink how intellectual property law works in Internet transactions and examine emerging new norms in this respect;
- facilitate the creation of effective online systems to resolve disputes; and
- coordinate and ensure the development of efficient and consistent responses to common concerns across national and multi-sectoral boundaries.

1.10 ACTIVITY

Enumerate the international organizations involved in E-commerce? (800-1000 words)

Unit 2: Overview of Entities and NGO's Involved in E-Commerce

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 National or Regional entities heavily involved in E-Commerce law

1.3 NGO's involved in E-Commerce law

1.4 E-Commerce Laws

1.5 Let's sum up

1.6 Further reading

1.7 Check your progress: Possible answers

1.8 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- National or Regional entities involved in E-Commerce
- Different NGOs that are involved in E-Commerce
- E-Commerce Laws

1.2 NATIONAL OR REGIONAL ENTITIES HEAVILY INVOLVED IN E-COMMERCE LAW

a) EUROPEAN UNION (EU)

What are the most important European Union e-commerce law directives?

The European Commission has shaped e-commerce law throughout Europe and around the world since the mid-1990s. Essential directives include:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market ("Directive on electronic commerce")
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.[236]

b) COUNCIL OF EUROPE

Who sits on the Council of Europe?

Although it is frequently confused with the European Union, the Council of Europe is a distinct body that encompasses a far larger group of countries than the EU. It includes 41 countries from Andorra to the United Kingdom. Several non-European countries, including the United States, Canada and Japan, enjoy observer status with the Council.

What is the Council's involvement with e-commerce issues?

The Council of Europe is best known for having successfully completed negotiations on a global cybercrime treaty in 2001. The treaty covers a wide range of online criminal activity, including fraud and computer hacking. It also addresses Internet service provider liability and copyright concerns. In late 2001, the Council announced plans to develop an additional protocol dealing with racism and xenophobia online.[237]

[236]Chauhan, Pratibha& Sharma, Pooja&Chauhan, Rahul & Jain, Ayushi. (2019). National eCommerce Policy: What India's new (Draft) eCommerce Policy outlines for Online Retailers and its Regulatory aspects. International Journal of Drug Regulatory Affairs

[237]MohanadHalaweh, Adoption of Ecommerce in Jordan: Understanding the Security Challenge , *The Electronic Journal of Information Systems in Developing Countries*, 47, 1, (1-13), (2017)

c) APEC

What is APEC?

The Asia-Pacific Economic Cooperation (APEC) was established in 1989 in response to the growing interdependence of Asia-Pacific economies. It began as an informal ministerial-level dialogue group with 12 members and has grown to include 21 member economies comprising some 2.5 billion people, a combined gross domestic product of over USD 18 trillion in 1999 and over 47 per cent of world trade. Its goal is to advance economic dynamism and sense of community within the Asia-Pacific region.[238]

APEC operates by consensus. The APEC chair rotates annually among members and hosts an annual ministerial meeting of foreign and economic ministers. At each year's ministerial meeting, members define and fund the work programmes for APEC's various committees, subcommittees, working groups and forums. APEC also has a Business Advisory Council composed of up to three senior business people from each member economy to provide advice on APEC action plans and specific business/private sector priorities.

What does APEC do?

APEC's goal is to achieve "free and open trade and investment in the Asia-Pacific by 2010 for developed member economies and 2020 for developing ones." In Osaka in 1995, APEC leaders established the three pillars of APEC activities: trade and investment liberalization, business facilitation and economic and technical cooperation. In 2000, APEC's objectives included:

- managing globalization through economic and technical cooperation and through participating in international forums;
- an Action Agenda for the New Economy, focusing on an e-Commerce Readiness Assessment, paperless trading and capacity building for both people and institutions;
- ensuring individuals from rural and urban communities alike have access to the Internet by 2010, including a pledge to triple the number of people with such access by 2005; and
- strengthening the multilateral trading system through a new WTO round.

[238] <http://www.apecsec.org.sg>

What is APEC's involvement with e-commerce?

APEC's E-Commerce Steering Group is currently working on a range of issues, including:

- a Digital Divide Blueprint for Action to address issues of the digital divide and reliable, affordable access to the information infrastructure;
- paperless trading;
- a review of the 2000 APEC Action Plan to Support the Use of Electronic Commerce by SMEs;
- development of APEC voluntary online consumer protection principles;
- development of policy regarding the creation of an environment conducive to e-learning; and
- reviewing and updating the 1998 APEC Blueprint for Action on Electronic Commerce.[239]

d) UNITED STATES

Which United States agencies and organizations have been at the forefront of e-commerce law and policy development?

The United States has been a leader in developing e-commerce law policy since the Internet's inception. Agencies and organizations leading the way include:

- The Department of Commerce, which continues to play an oversight role over the Internet's infrastructure including the domain name system;
- The Federal Trade Commission, which has played the role of privacy and consumer protection enforcer;
- The Department of Justice, which administers United States competition law policy;
- The State Department, which leads the United States delegation at the Hague Conference negotiations;

[239]Teegen, Hildy&Doh, Jonathan &Vachani, Sushil. (2004). The Importance of Nongovernmental Organizations (Ngos) in Global Governance and Value Creation: An International Business Research Agenda. Journal of International Business Studies

- The Federal Communications Commission, which regulates communications infrastructure;
- The American Bar Association, which has developed policy documents on jurisdiction, privacy and e-commerce law; and
- The National Conference of Commissioners on Uniform State Law, which has drafted the Uniform Electronic Transactions Act, the United States version of the UNCITRAL Model Law on Electronic Commerce.

e) CANADA

Who regulates e-commerce activity in Canada?

No single agency or entity can be said to regulate the Internet or e-commerce in Canada. Agencies that play a significant role in Canadian Internet and e-commerce law and policy include:

- Industry Canada (privacy, electronic commerce, electronic signatures, copyright)
- Justice (jurisdiction, cybercrime)
- Canadian Heritage (copyright)
- Competition Bureau (consumer protection, marketplace regulation)
- Canadian Internet Registration Authority (dot-ca domain names)
- Canadian Copyright Board (copyright)
- Canadian Radio-television and Telecommunications Commission (broadcast, Internet regulation)
- Uniform Law Conference of Canada (e-commerce, jurisdiction).

f) AUSTRALIA

What is the most prominent e-commerce regulatory activity in Australia?

Although Australia has enacted e-commerce, privacy and online gambling legislation, it is perhaps best known for its online content regulation. The Australia Broadcasting Authority has been granted the power to order offensive content removed from Australian-based websites and to request that Australian Internet service providers take steps to make such foreign-based

content inaccessible to Australian users. Despite dire predictions about the likely effect of such legislation, few sites have been removed from the web, and the number of complaints has been relatively limited.

g) SINGAPORE

How early did Singapore adopt e-commerce legislation

While dozens of countries have enacted e-commerce legislation, Singapore stands as one of the very first to establish an e-commerce legal framework. The country enacted the Electronic Transactions Act of 1998 in June of that year. Moreover, the first digitally signed international government document between Singapore, Canada and the State of Pennsylvania was signed in April 1998.[240]

h) COLOMBIA

Has Columbia enacted e-commercelegislation?

Yes. Colombia approved a law on electronic commerce, digital signatures and certification authorities (Proyecto de Ley SobreComercioElectrónico, FirmasDigitales y Autoridades de Certificación) in August 1999. The law is based on the UNCITRAL Model Law on Electronic Commerce. Further regulations concerning requirements for certificate authorities (discussed further below) have also been adopted.

i) ARGENTINA

Is it too late to adopt e-commerce legislation at the national level?

No. While much of Europe, the United States and Canada have enacted their legislation, and many countries are still working on appropriate domestic e-commerce statutes. For example, Argentina enacted its digital signature law in December 2001. The Argentinian law addresses the licensing and liability of certificate authorities and the legal effects of electronic documents signed by digital signature. Moreover, the Government has prepared amendments to the Civil Code in order to adjust requirements of form to electronic commerce.

[240]INTERNATIONAL TELECOMMUNICATION UNION
<https://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc>

j) TUNISIA

How broad is Tunisia's e-commerce legislation?

Tunisia enacted the Electronic Exchanges and Electronic Commerce Law in 2000. Much like its counterparts around the world, the law covers electronic contracting and the validity of electronic signatures. In addition, the law boldly creates a National Agency for Electronic Certification, an administratively independent public agency designed to address electronic signature and certification issues.

1.3 NGOs INVOLVED IN E-COMMERCE LAW

a) GLOBAL BUSINESS DIALOGUE ON E-COMMERCE (GBDE)

Who belongs to GBDe?

Established in January 1999, the Global Business Dialogue on E-commerce counts dozens of the world's largest companies as its members including Disney, Vivendi Universal, BCE, AOL Time Warner, NEC, NTT, Hitachi, Toshiba, Alcatel, Deutsche Telkom, Daimler Chrysler and Nokia.[241]

What are GBDe's areas of concern?

GBDe focuses on providing governments with a business perspective on e-commerce law and policy development. The organization has identified eight areas of concern: consumer confidence, convergence, cybersecurity, digital bridges, e-government, intellectual property rights, taxation and trade.[242]

b) INTERNET LAW & POLICY FORUM (ILPF)

What is ILPF?

Founded in 1995, the Internet Law and Policy Forum is an international non-profit organization of major, Internet-oriented companies, including Verisign, Microsoft, BCE, Fujitsu and Deutsche Telekom, dedicated to promoting the global growth of electronic commerce and communications

[241] Al-Qirim, Nabeel (2007) The adoption and diffusion of e-commerce in developing countries: The case of an NGO in Jordan. Information Technology for Development

[242] Brinkerhoff, D.W. and Brinkerhoff, J.M. (2002) 'Government– non-profit relations in comparative perspective: evolution, themes, and new directions', Public Administration and Development 22(1): 3–18

by contributing to solutions of the particular legal issues which arise from the cross-border nature of the Internet and electronic networks. ILPF provides information, calling upon the legal, business and technical expertise of its member companies and other companies, from governments and intergovernmental organizations and from the practice of law around the world.

What are ILPF's key issues?

ILPF addresses issues of concern through working groups consisting of representatives from member organizations. It currently has four such working groups:[243]

- Working Group on Jurisdiction
- Working Group on Electronic Authentication (a combination of the original Working Groups on Certificate Authorities and on Digital Signatures)
- Working Group on Content Regulation and Intermediary Liability
- Working Group on Self-Regulation.

c) CONSUMERS INTERNATIONAL

What is Consumers International?

Founded in 1960, Consumers International supports, links and represents consumer groups and agencies all over the world. It has a membership of more than 260 organizations in almost 120 countries. It strives to promote a fairer society through defending the rights of all consumers, including the poor, marginalized and disadvantaged.[244]

How is Consumers International involved in e-commerce?

Consumers International identified e-commerce as an issue of concern in 1998, calling on governments to establish global protections for consumers who are engaged in e-commerce. Since that time, the organization has played a leading role in crafting e-commerce consumer protection policy and in working to establish effective and fair dispute resolution processes.

[243] Fowler, A (2001) The Virtuous Spiral: A Guide to Sustainability for NGOs in International Development,Earthscan Publications: London

[244] Brown, L.D. and Moore, M.H. (2001) 'Accountability, strategy, and international nongovernmental organizations', Nonprofit and Voluntary Sector Quarterly 30: 569–587

d) ELECTRONIC PRIVACY INFORMATION CENTRE (EPIC)

What is EPIC?

EPIC is a public interest research centre in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment of the United States Constitution and constitutional values.[245]

In what cases has EPIC become involved?

EPIC acts predominantly on cases of interest to the United States. It has appeared on some of the Internet and e-commerce's leading-edge cases including the Scarfo case on keystroke monitoring, the Microsoft antitrust case and the case challenging the constitutionality of the Children's Online Protection Act. EPIC has also played an important role in global awareness campaigns involving privacy issues.

e) INTERNATIONAL CHAMBER OF COMMERCE (ICC)

What is ICC?

The International Chamber of Commerce is a world business organization that speaks on behalf of enterprises from all sectors in every part of the world. ICC promotes an open international trade and investment system and the market economy. It often works with its member companies to develop global business codes of conduct. It also provides essential services, foremost among them the ICC International Court of Arbitration, a leading arbitral institution. Within a year of the creation of the United Nations, ICC was granted consultative status at the highest level with the United Nations and its specialized agencies.

How is ICC involved in e-commerce law and policy?

ICC is involved in e-commerce law issues on several fronts. Given its leading role in dispute resolution, ICC has shown a keen interest in developing dispute resolution for both B2C and B2B e-commerce. It has adapted for e-commerce its leading international trade rules, such as the Incoterms and the Uniform Rules for Documentary Credits (UCP 500). The organization has also become involved in jurisdictional negotiations, privacy and electronic contracting.

[245] Fisher, J (1998) Nongovernments: NGOs and the Political Development of the Third World, Kumarian Press: West Hartford, CT

1.4 E-COMMERCE LAWS

(i) UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

1 ORIGINS

The Model Law, adopted in 1996, is intended to facilitate the use of modern means of communication and storage of information, such as electronic data interchange (EDI), electronic mail and telecopy, with or without the use of such support as the Internet. It is based on the establishment of a functional equivalent for paper-based concepts such as "writing", "signature" and "original".[246]

2 KEY PROVISIONS

How does the Model Law treat electronic transactions?

The key principle underlying the Model Law is the concept of "electronic equivalence," found in Article Five. Although the Model Law does not deem electronic communications valid (just as with paper documents, legal validity depends upon more than a document's form), it provides that information or documents will not be denied legal effect or enforceability solely because they are in electronic format.

How does the Model Law achieve electronic equivalence?

A series of functional equivalency rules specify what conditions must be met for electronic communication to constitute a legally effective substitute for a conventional, paper-based communication. For example, Article Six provides that a legal requirement to provide information or a document sent "in writing" is satisfied by its electronic equivalent if it is in a form that can be subsequently accessed and used by the recipient.[247]

Article Eight states that electronic documents will satisfy a legal requirement for "original" documents if there is a reliable assurance as to the integrity of the information and that the information is capable of being displayed to the person to whom it is to be presented. The

[246]Arnove, R F and Christina, R (1998) 'NGO–state relations: an argument in favor of the State and complementarity of efforts', Current Issues in Comparative Education 1(1): 1–5

[247]Boli, J and Thomas, GN (eds) (1999) Constructing World Culture: International Nongovernmental Organizations Since 1875, Stanford University Press: Stanford, CA

question of whether an assurance is reliable is to be determined in the light of all the circumstances, including the purpose for which the document was created.[248]

How is the integrity of the information determined?

Article Eight also addresses this issue. It provides that the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

Does the Model Law address the admissibility and evidential weight of electronic communication?

Yes. Article Nine creates an electronic equivalence standard for evidentiary purposes as it provides that evidentiary rules shall not deny the admissibility of an electronic communication solely on the grounds that it is in electronic form.

What conditions does the Model Law set for data retention?

Article Ten addresses the issue of data retention. It provides that data retention requirements are met where the information contained with the electronic message is accessible so as to be usable for subsequent reference, the message itself is retained in the format in which it was generated and any information indicating origin, destination, date and time of the message are retained.

Does the Model Law address online contracts?

Yes. The most interesting section of the Model Lawfocuses on online contracts. Although thousands of contracts are entered into daily through the Internet, some sellers and consumers remain uncertain of the legal implications of clicking the "I agree" button on a website. Article Eleven of the Model Lawremoves any doubt that this popular form of online consent is valid by stipulating that unless the parties agree otherwise, an offer or acceptance of an offer can be expressed in electronic form.

1.5 LET'S SUM UP

[248] <https://www.cl.cam.ac.uk/teaching/1314/ECommerce/Batch2.pdf>

In this chapter, we have studied the varied national and regional entities heavily involved in E-Commerce Laws along with different NGOs involved in E-Commerce Laws. Finally, we ended the discussion with the origin of UNCITRAL Model Law and the key provisions with respect to it.

1.6 FURTHER READING

- Deloitte Research study on E-commerce in India.https://www2.deloitte.com/in/en/pages/technology-media-and telecommunications/articles/Ecommerce-in-india.html
- Amith, Mr & MA, Amith& Professor, Asst. (2012). E-commerce: Opportunities and Challenges (ISBN:978-81910530-3-6).
- Study by Forrester Research: India growing fastest in E-commerce. https://yourstory.com/2017/02/E-commerce-forrester-research/
- Understanding the challenges in cross border E-commerce by AjeetKhurana Feb 4, 2014. http://blogs.pb.com/ecommerce/2014/02/04/understanding-challenges-cross-border-ecommerce/

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) Name 5 national or regional entities involved in E-Commerce Law?

- European Union
- Council of Europe
- Canada
- Singapore
- Argentina

2) How was Consumers International involved in E-Commerce?

Consumers International identified e-commerce as an issue of concern in 1998, calling on governments to establish global protections for consumers who are engaged in e-commerce.

Since that time, the organization has played a leading role in crafting e-commerce consumer protection policy and in working to establish effective and fair dispute resolution processes.

3) What is Internet Law and Policy Reform?

The Internet Law and Policy Forum is an international non-profit organization of major, Internet-oriented companies, including Verisign, Microsoft, BCE, Fujitsu and Deutsche Telekom, dedicated to promoting the global growth of electronic commerce and communications by contributing to solutions of the particular legal issues which arise from the cross-border nature of the Internet and electronic networks.

4) When was UNCITRAL Model Law adopted?

The Model Law was adopted in 1996.

1.8 ACTIVITY

Explain the National entities and NGOs involved in E-Commerce along with the features of UNCITRAL Model Law? (1000 words)

Unit 3: Implementation of Model Law and Development in India

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 National Implementation of UNCITRAL Model Law

1.3 E-Governance in developed and developing countries

1.4 International instruments on E-Contract

1.5 Current Status of MSMEs & E-Commerce development in India

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- National Implementations of UNCITRAL Model Law
- International instruments on E-Contract
- Current Status of MSMEs & E-Commerce development in India

1.2 NATIONAL IMPLEMENTATION OF UNCITRAL MODEL LAW

a) UNITED STATES

Has the United States implemented the UNCITRAL Model Law at the national or state level?

Yes, both. Nevertheless, most of the activity initially occurred at the state level, with dozens of states using the Uniform Electronic Transaction Act (UETA), developed by the National Conference of Commissioners on Uniform State Law, as a model. When some state laws began

to deviate from UETA, the United States Congress stepped in to create a uniform standard by enacting the Electronic Signatures in Global and National Commerce Act (E-SIGN) in 2000.[249]

Are there any important differences between the UETA and the UNCITRAL Model Law?

Yes. First, UETA includes a consent provision that clarifies that the Act does not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form. Second, it facilitates the use of electronic signatures for notarization of documents. Third, Section 10 of UETA features rules for where a change or error in an electronic record occurs in a transmission between parties to a transaction.

How does E-SIGN co-exist with the state law versions of UETA?

E-SIGN specifically provides that if there is a modification to UETA, state statutes that incorporate that modification supersedes the federal statute.

What are some of the provisions that distinguish E-SIGN from UETA?

First, E-SIGN includes strong consumer consent provisions. These provisions require that consumers affirmatively consent before electronic records can be used to provide them with information that, under other law, must be provided or made available to them in writing. Consumers are also granted the right to withdraw their consent.[250]

Second, E-SIGN contains some fairly expansive provisions related to contracting by electronic agents. The statute provides that a contract may not be denied legal effect solely because its formation or creation involved one or more electronic agents, provided that the action of the electronic agent is "legally attributable" to the person to be bound.

b) EUROPEAN UNION

Has the European Union addressed the issues found in the UNCITRAL Model Law?

Yes. The EU's Electronic Commerce Directive contains several articles that bear direct similarity to principles found in the Model Law. Although it falls to Member States to implement the

[249] INTERNATIONAL TELECOMMUNICATION UNION <https://www.itu.int/ITU-T/special-projects/ip-policy/final/Attach04.doc>

[250] Al-Hakim L, Global E-government: Theory, Applications and Benchmarking, University of South Queensland, Australia, published in Hershey PA, London, 2006

directive into national law, the directive does have a direct effect in those states that fail to enact e-commerce legislation in a timely manner.[251]

How does the E-commerce directive treat electronic contracts?

Article 10 of the directive speaks to contracts concluded by electronic means. It provides that Member States shall ensure that their legal system allows contracts to be concluded by electronic means. In particular, Member States are warned not to create obstacles for the use of electronic contracts.[252]

c) CANADA

Has Canada implemented the UNCITRAL Model Law on e-commerce into national law?

Yes and no. Although the Model Law has not been enacted into federal law, with one exception, all provinces and territories have enacted versions of a Canadian model based on the United Nations model.[253]

What is the Canadian model law?

The Uniform Electronic Commerce Act(UECA), a project of the Uniform Law Conference of Canada (ULCC), obtained official approval in 1999, providing Canada with a legal model for electronic commerce transactions. The subject of more than two years of negotiation, UECA brought much-needed certainty to the world of e-commerce. Based largely on the UNCITRAL Model Law, it clarifies issues such as the enforceability and formation of online contracts, the use of electronic agents in the contracting process and at what point an electronic contract is presumed sent and received.[254]

Have all provinces and territories enacted the Canadian model into law?

Not quite. UECA has received widespread approval from Canadian provinces and territories. As of March 2002, all Canadian provinces, with the exception of Quebec, had enacted legislation based on the UECA model. In November 2001, Quebec enacted its own e-commerce legislation that departs from the UECA model.

---

[251] Asian Development Bank Institute (2005). Designing e-Government for the poor. Bangkok, Thailand

[252](Uncitralrcap.org, 2020)
<http://uncitralrcap.org/wp-content/uploads/2015/11/session3_Ciccu-Mukhopadhaya.pdf>

[253] Chen, P (2008) Electronic Governance. Oxford Companion to Australian Politics/Oxford Reference Online B Galligan and W Roberts, Oxford University Press

[254] United Nations, "E-government Strategy Report;" New York, 2002

d) OTHER COUNTRIES

What other countries have enacted the UNCITRAL Model Law into national law?

Dozens of countries from virtually every continent worldwide have used the Model Law as the basis for establishing national e-commerce legislation.

In South America, **Colombia** passed the Electronic Commerce Law 527 in 1999, based on the 1996 UNCITRAL model law. It establishes the validity and admissibility for "data messages," as well as the enforceability of contracts that contain data messages. Additionally, it provides for the validity of digital signatures and delineates standards for the licensure of certification entities and for the issuance of certificates.

In Asia, **Thailand** also passed its own Electronic Commerce Law in 1999. It addresses electronic signatures along with all electronic communications.

In the Americas, **Bermuda** enacted the Electronic Transactions Act in 1999 to address the legal validity and enforceability of electronic signatures and records as well as their admissibility as evidence in any legal proceeding.[255]

In Africa, **Tunisia** enacted the Electronic Exchanges and Electronic Commerce Law in 2000. Although the law addresses the general organization of electronic exchanges, it also governs electronic contracts including the validity and execution liability that may arise from that form of contract.

1.3 E-GOVERNANCE IN DEVELOPED AND DEVELOPING COUNTRIES

E-Governance has become popular worldwide in present time.[256] To make working of government more efficient, responsive and transparent many developed and developing countries

[255]Ndou V, "E–Government for Developing Countries: Opportunities and Challenges," EJISDC: The Electronic Journal on Information Systems in Developing Countries,Vol 18, No 1, pp 1- 24,2004

[256]E-Governance: Past, Present and Future in India
<https://arxiv.org/pdf/1308.3323>

have taken some useful steps for the expansion of e-governance in their respective countries.[257] Countries which are in the race of e-governance implementation are UK, USA, New Zealand, Brazil etc. Below the following countries with their respective projects has been described:

UNITED STATES OF AMERICA

On July 18, 2001, Task Force to identify priority actions that achieve strategic improvements in government and set in motion a transformation of government around citizen needs was done.[258]

VARIOUS PROJECTS

1. Recreation One-Stop: This project was started on 31 April 2002. It aimed to:

- Agreement with private sector reached on implementation of new recreation online projects.
- Additional recreation projects available online.

2. EZ Tax filling: This project was started on 31april, 2002. It aimed to:

- Filling and refunding of taxes online.
- Initial deployment of industry partnership free e-filling solution for 2003 season.

3. Federal Assets Sales: started on 31 March 2003. It aimed to:

- Develop pilot business integration
- Re-host federal sales.

4. E-Payroll/HR: started on 31 March 2002. Aimed to:

- complete and submit business case to PMC
- integrated enterprise architecture

5. E-Authentication: started on 1 July 2002. Aimed at:

- Initial authentication gateway prototype
- Full deployment[259]

[257]Basu, Subhajit (2004) E-government and developing countries: An overview. INTERNATIONAL REVIEW OF LAW COMPUTERS & TECHNOLOGY

[258]E-governance International Status <https://bettersocietyblog.blogspot.com/p/governance-international-status.html>

UNITED KINGDOM

In April 2000, the Cabinet Office in the UK came out with the document 'E-Government: A Strategic Framework for Public Services in the Information Age'.

VARIOUS PROJECTS

1. Cornwall Electronic Health Record Pilot: this project was started in April 2000. It aimed to:

- Pan-community EHR demonstrator
- Connect all General Practitioners to NHSnet (national-level NHS Virtual Private Network or intranet)
- 24-hour emergency care record
- Common information architecture
- Condition-specific care modules – mental health, coronary heart disease, diabetic care

2. Go-between Project: this project is for Calne Community Area in Wiltshire. This project is designed to assist a local rural community to organize its transport services by identifying unmet local demand and matching it with spare capacity.

3. Plymouth Bus Project: Commissioned by Plymouth City Council to undertake a comprehensive study of the bus network and propose initiatives for its future development and investment. (Completed in January 2009)

4. Integrating Transport: Started in South West Hertfordshire. Lead consultant on a project commissioned by Watford Borough Council. Preparation of a sustainable transport strategy for implementation over the next ten years. (Completed October 2008)[260]

NEW ZEALAND

[259]Nawafleh, Sahem&Obiedat, Ruba&Harfoushi, Osama. (2012). E-Government Between Developed and Developing Countries. International Journal of Advanced Corporate Learning (iJAC)

[260] Deloitte and Touche 'At the dawn of e-government: the citizen as customer' Available at <www.publicnet.co.uk/publicnet/fe000620.htm>

In May 2000, Realising the importance of opportunities offered by ICT, the New Zealand Government came out with its e-government vision document and an 'E-Government Unit' was established by the State Services commission.[261]

VARIOUS PROJECTS

The Treaty of Waitangi: It is the founding document of New Zealand. This website, launched in 2003, to provide information and resources for an informed understanding and greater public knowledge of the treaty.

As people's want advancement in their lifestyle same they want in their government. Success or failure of any government depends on three things:

- The way the government works.
- Transparency in its working and information.
- Communication to its citizen.

In developing countries, the Government beneficiary scheme can be reached to the lowest pyramid of society efficiently by implementing E-Governance projects. It can bridge the gap between rich and poor.[262]

E-GOVERNANCE

Use of internet by the government to provide its services at the doorstep of customers, business and other stakeholder.

In E-Governance, the government makes the best possible use of internet technology to communicate and provide information to common peoples and businessman. Today, electricity, water, phone and all kinds of bills can be paid over the internet. All this is what government and citizens are using and doing. All are dependent on internet and when citizens depends on government internet services all that comes is E-Governance.

---

[261] M Backus 'E-governance in developing countries', IICD Research Brief No 1, March 2001 <www.iicd.org>

[262] P Norris 'The worldwide digital divide: information poverty, the Internet and development' Harvard University, 2000 Available from <http:// www.ksg.harvard.edu/iip/governance/psa2000dig.pdf>

There are four pillars of E-Governance:

1. CONNECTIVITY: Connectivity is required to connect the people to the services of the government. There should be strong connectivity for effective e-governance.

2. KNOWLEDGE: Here knowledge refers to IT knowledge. The government should employ skill full engineers who can handle the e-governance in an efficient way. These engineers also handle all kind of fault that may occur during the working of e-governance.[263]

3. DATA CONTENT: To share any knowledge or information over the internet, there should be its database. This database should have the data content which is related to government services.

4. CAPITAL: Capital can be on public or private partnership. It refers to money used by the government to provide their services or to that sector of the economy based on its operation.

1.4 INTERNATIONAL INSTRUMENTS IN E-CONTRACT

1. THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) MODEL LAW ON ELECTRONIC COMMERCE

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce was promulgated in 1996 (and amended in 1998) to assist countries in the framing of legislation which would enable and facilitate electronic commerce and electronic government. Surprisingly, it makes no reference to the Internet.[264]

This model law establishes rules and norms that validate and recognize contracts formed through electronic means, sets rules for forming contracts and governing electronic contract performance, defines the characteristics of valid electronic writing and an original document, provides for the

[263]Description about E-Governance
<https://bisma.in/description-about-e-governance/>
[264]UNCITRAL Model Law on Electronic Commerce | The IT Law
<https://itlaw.wikia.org/wiki/UNCITRAL_Model_Law_on_Electronic_Commerce>

acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings.[265]

The Model Law adopts a limited framework approach. It is not intended to be a comprehensive, code-like articulation of the rules for electronic transactions, nor is it intended to govern every aspect of electronic contracting. Instead, it is intended to enable and facilitate electronic commerce by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it was intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade.

The underlying analytical approach of the Model Law is the "functional equivalence" approach. This approach evaluates the underlying purposes and functions of traditional paper-based legal requirements and assesses to what extent electronic transactions can meet these purposes and functions. Where electronic transactions can satisfy the purposes and functions, the Model Law requires that they be given equal status. In effect, it puts electronic communications on par with traditional paper-based modes of communication.

Therefore, rather than rewriting the law, the Model Law seeks to extend the scope of standard national legal definitions of "writings", "signatures" and "originals" to encompass their electronic counterparts. It provides that information is not to be denied legal effect merely because it is in electronic form or is signed electronically. It also deals with transmission and receipt of messages and contracts for the carriage of goods. It does not address jurisdictional or conflict of laws issues.

2. MODEL LAW ON ELECTRONIC SIGNATURES

Building on the success of the Model Law as a precedent for national law reform, UNCITRAL adopted in 2001 a Model Law on Electronic Signatures, which builds on the signature provision in the 1996 Model Law. From a legal and security perspective, signatures provide two key

[265]Martin, Charles H., The Electronic Contracts Convention, the CISG, and New Sources of E-Commerce Law Tulane Journal of International & Comparative Law, Vol 16, No 2, Spring 2008

elements –authentication and integrity.[266] The use of such of such techniques is seen as critical to the widespread adoption of electronic commerce, particularly in terms of meeting the requirements of Governments and regulatory authorities.

3. UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS

The Convention was prepared by the United Nations Commission on International Trade Law and adopted on 11 April 1980. It came into force on 1 January 1988. The Convention has currently 85 member States. The purpose of the Convention is to provide a modern, uniform and fair text of the law for contracts for the international sale of goods, reduce barriers in international trade and promote the use and development of international trade. The Convention thus contributes significantly to introducing certainty in commercial exchanges, decreasing transaction costs and facilitates the ease of trading across borders. The Convention governs the international sale of goods between private businesses, excluding sales to consumers, sales of services and sales of specified types of goods. The Convention consists of 101 articles which are divided into four parts.[267]

1.5 CURRENT STATUS OF MSMEs & E-COMMERCE DEVELOPMENT IN INDIA

- **E-COMMERCE SIZE IN INDIA**

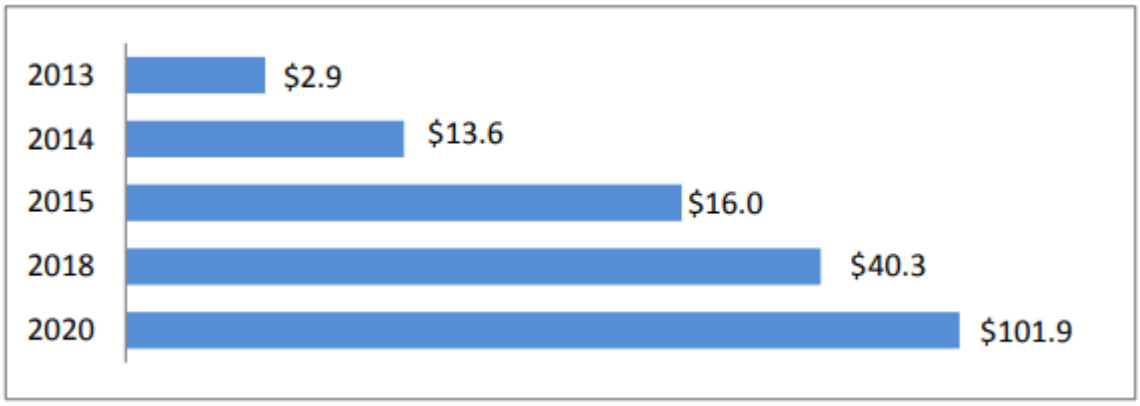
The E-commerce business is expected to form the largest part of Indian economy with a value of approximately USD 100 billion by 2020. E-commerce is facilitating MSMEs to scale up their operations by providing a means of financing, technology and training. Evolution of technology-

[266] A. Introduction B. EDI and trading partner <https://unctad.org/en/Docs/sdteecb20061ch8_en.pdf>

[267] UN agreement to benefit Fiji economy - Post Courier <https://postcourier.com.pg/un-agreement-to-benefit-fiji-economy/>

led innovations such as digital payments, hyper-local logistics, mass customer engagements and digital advertisements have enabled the E-commerce industry to grow speedily.[268]

Within the E-commerce industry, the Gross Merchandise Value (GMV) is an important metric for valuations, especially during the early stages of growth. The majority of B2C E-commerce companies report low profitability even in developed economies, and the situation in India is no different. While the GMV is rising, the companies have to suffer an overall loss as the Ecommerce companies establish themselves. The GMV for B2C segment in India was approximately USD 16 billion in 2015.

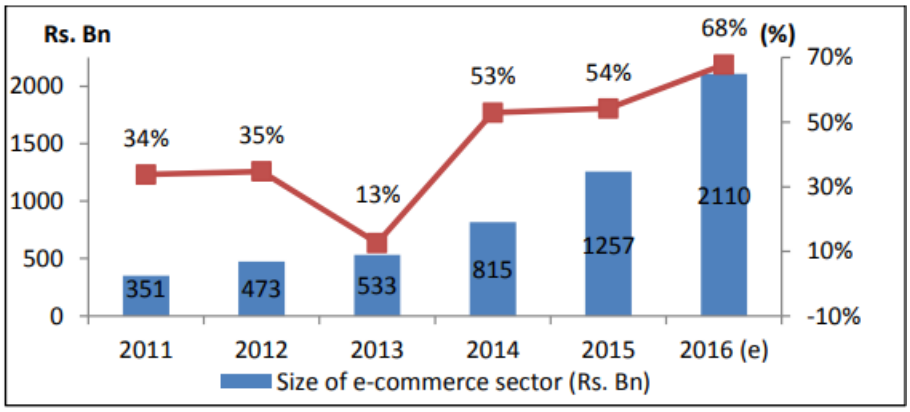


E-commerce size ($ billions) in India

As per another report, the value of E-commerce sector (GMV) in Indian rupees was as under:-

- The size of the E-commerce industry was estimated to be Rs. 2,110 billion by 2016 as per Digital Commerce Report 2015 (IAMAI and IMRB). The industry was worth Rs. 351 billion in 2011 and grew at a CAGR of 37% to touch Rs. 1,257 billion in 2015.

[268] International Journal of Management and Economics <http://ijme.co.in/paperadmin/images/files/Fle_1533560850.pdf>



Size of E-Commerce Sector (2011-2016)

MSMEs in India have been generally operating in a traditional manner and have been dependent on domestic trading activities. But, with a growing rate of internet penetration, MSMEs are also gradually changing their operations to avail the opportunities to trade through E-commerce. A large number of MSMEs is now involved in online transactions. These MSMEs look towards an enhanced customer base and increased profits by using E-commerce technology. MSMEs believe that use of E-commerce will boost their business growth.

- **GROWTH OF B2B E-COMMERCE IN INDIA**

The growth of the B2B E-commerce segment is relatively slower compared to the B2C e-commerce segment in India. This is because the entry barriers in the B2B E-commerce are more than those in the B2C E-commerce industry.[269] A B2B E-commerce company has to have a strong business model, long term logistical arrangements with rail, road and ports and also adhere to stringent regulatory and taxation laws. With an aim to tap the huge potential in the B2B E-commerce market in India, apart from the existing B2B companies, leading B2C companies have also started to build their own platforms for small business owners and traders. This is expected to be supported by rising expectations among a growing number of companies buying and selling online and a shift to conduct procurement transactions through the Internet.

[269] e-Commerce in India A Game Changer for the Economy <https://slidelegend.com/e-commerce-in-india-a-game-changer-for-the-economy_59b65b061723ddf2725f0bde.html>

Understanding this untapped potential of the B2B E-commerce industry, the Government has allowed 100% FDI in B2B E-commerce, which has enabled globally successful B2B E-commerce companies such as Walmart and Alibaba to evince interest in the India B2B E-commerce industry.

- **RISE IN INTERNET USERS GIVING FILLIP TO E-COMMERCE**

In 2014, the number of internet users in India stood at around 280 million, and it was estimated that the number would rise to around 640 million by 2019. An increase of almost 70 million Internet users in a year is very significant. The rise of mobile internet users is also expected to touch 457 million by 2019. Comparing this with the projected growth, the E-commerce in India by the year 2020 is expected to touch USD 100 billion.

- **MERGERS AND ACQUISITIONS IN E-COMMERCE INDUSTRY**

E-commerce companies in India have also witnessed consolidation in the past 2-3 years. Larger E-commerce companies have been acquiring smaller companies to either diversify their product range or to enhance business operations. Such mergers and acquisitions have mainly centered on companies in the logistics, payment solutions and digital advertising areas. It is estimated that a total of 930 M&A deals with a cumulative value of USD 26.3 billion took place in India in 2015, of which, 259 deals worth USD 2.43 billion pertained to the E-commerce industry. Also, many strategic deals took place in the hyper-local, food-tech and real estate listing segments.[270]

- **PRIVATE ENTITY/VENTURE FUNDING OF E-COMMERCE COMPANIES IN INDIA**

Private equity and venture fund investments reached an all-time high in 2015 at USD 20 billion in India. The key sectors that saw investments were Information Technology, with 666 deals worth USD 4.49 billion, followed by consumer goods with 280 deals worth USD 4.69 billion.

[270] Kierkegaard, Sylvia (2008) E-Contract Formation: U S And EU Perspectives

The majority of these investments have been concentrated in e-tailing (70% of investment), followed by online classifieds (17%) and lastly online travel and taxi (9%). This aggressive drive comes at a point when capital is becoming scarce for top venture-backed online retail companies.[271] There is also a reduction in the dependence on discounts as a growth strategy. Investors are currently focusing on start-ups that may scale slowly but have sound fundamentals and strong business models. In essence, these start-ups should have the ability to survive any scenario. Therefore, investors, today are interested in start-ups in sectors like health care and education which, by the nature of their offerings, will provide sustainable models and create legacy firms.

1.6 LET'S SUM UP

In this chapter, we have studied the National Implementation of UNCITRAL Model Law along with E-Governance in developed and developing countries. We also studied the International instruments on E-Contract and finally, we ended the discussion with the current status of MSMEs & E-Commerce development in India.

1.7 FURTHER READING

- Annual Report 2015-16, of Ministry of MSME, Govt. of India. http://msme.gov.in/relatedlinks/annual-report-ministry-micro-small-and-medium-enterprises
- Ministry of Micro, Small and Medium Enterprises, Govt. of India site: msme.gov.in http://msme.gov.in/
- International Journal of Computer Applications (0975 – 8887) Volume 53– No.7, September 2012

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

[271](Scholarlycommons.law.northwestern.edu, 2020) <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1015&context=njtip>

1) **Name 3 countries that have implemented the Model Law?**

- United States
- Canada
- European Union

2) **What are the four pillars of E-Governance?**

- Connectivity
- Knowledge
- Data Content
- Capital

3) **Name any 2 E-Governance projects executed by the UK?**

- Go-between Project
- Plymouth Bus Project

4) **Give a brief about the present status of MSMEs?**

The E-commerce business is expected to form the largest part of Indian economy with a value of approximately USD 100 billion by 2020. E-commerce is facilitating MSMEs to scale up their operations by providing a means of financing, technology and training. Evolution of technology-led innovations such as digital payments, hyper-local logistics, mass customer engagements and digital advertisements have enabled the E-commerce industry to grow speedily. Within the E-commerce industry, the Gross Merchandise Value (GMV) is an important metric for valuations, especially during the early stages of growth. The majority of B2C E-commerce companies report low profitability even in developed economies, and the situation in India is no different. While the GMV is rising, the companies have to suffer an overall loss as the Ecommerce companies establish themselves. The GMV for B2C segment in India was approximately USD 16 billion in 2015.

1.9 ACTIVITY

Elucidate how UNCITRAL Model Law has been implemented by different countries along with the E-Governance development in developed and developing countries? (800 – 1000 words)

Unit 4: Dark Web and International Cyber Laws

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Basic understanding and definitions

1.4 Danger and Crimes in Dark Web

1.5 Laws across different jurisdictions

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Basic understanding of Dark web and its concepts
- Danger and Crimes in Dark Web
- Laws across different jurisdictions

1.2 INTRODUCTION

The influx of digital technologies and the digitalisation of modern society have introduced both challenges as well as prospects for law enforcement. With the advent of technology, the face of crime also evolves and makes it extremely challenging for the authorities to keep up. The pace of the technology advancement is much ahead of the pace to keep a check to it; therefore, mostly such advancements run unchecked and enter into the illegal boundaries of law and humanity. One such challenge has been the Dark Web (also known as Dark Net). As fancy and helpful the world of the web has proved to be, its misuse and criminal effects are equally debatable.

Presently, most of the focus is on the defies as crime-fighting has become beleaguered by a loss of access to data inclusive of location through the dark web.
The very understanding of dark web is like that of black market where all the prohibited, top-secret and exclusive information is available apart from illegal practices of child pornography, human trafficking, drug mafia, assassinators etc. An offender can commit a crime anywhere and at any time, parting behind a track of victims in diverse jurisdictions.

All the information unavailable in a public domain which is either extremely private, of national importance or security, of specific illegal acts, of privately-held details can be accessed, and all the illicit goods and services can be availed without having to disclose ones' identity. It is not only used for criminal activities but also other activities of journalism, national security, high-end research etc.

For beings living under oppressive regimes that block large portions of the Internet or penalise political disagreement, the dark web is a lifeline that provides access to information and safeguards from maltreatment. In liberated societies, it can be a precarious whistleblowing and communication tool that shields people from vengeance or judgment in the workplace or community. Otherwise, it can merely dispense privacy and anonymity for those wary of how corporations and governments are tracking, using, and potentially monetising their data. On the other side, the same privacy and anonymity that dispense protection from tyrants and targeted announcements also make the dark web a facilitator for the crime. Some of the more predominant illicit actions include arms trafficking, drug dealing and the contribution of abusive matter such as child pornography and images of viciousness and other varieties of abuse.[272]

Cybercriminals often choose to use the Dark Web to involve in illegal conduct. The Dark Web is packed with illicit marketplaces and platforms where criminal activity is advertised and communicated. There are search engines which are directed specifically to finding stuff on the Dark Web. The topmost of those are - Tor network - .onion and I2P - .i2p

[272]Digging through 3 layers to the dark web - CUInsight
<https://www.cuinsight.com/digging-through-3-layers-to-the-dark-web.html>

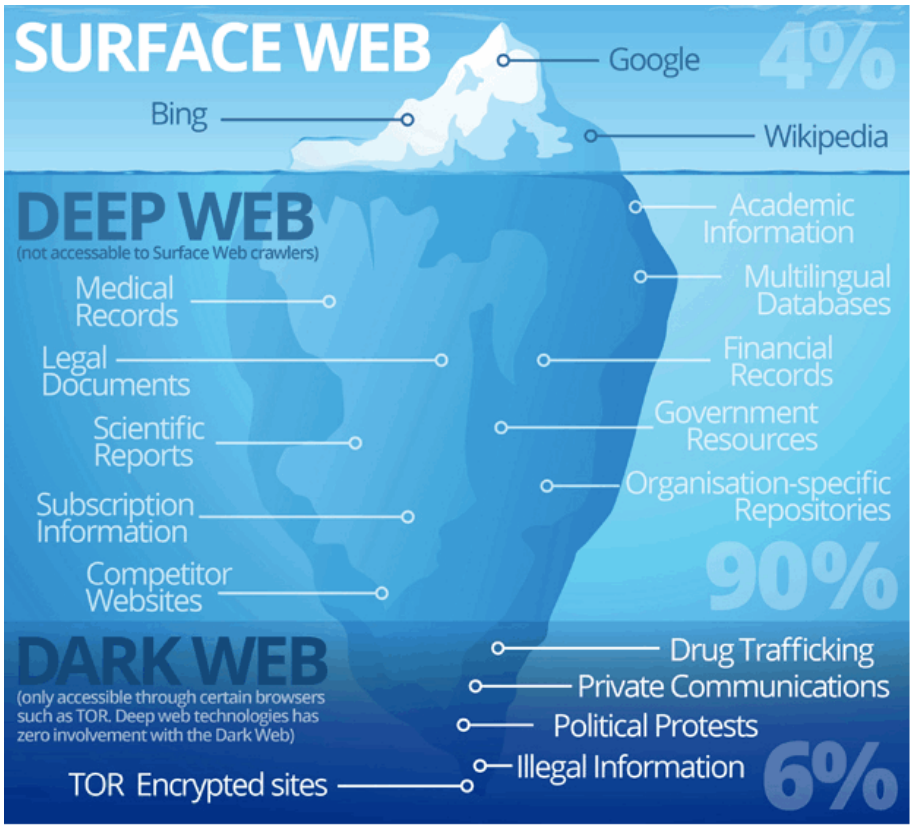
1.3 BASIC UNDERSTANDING AND DEFINITIONS

The definition as per the **United Nations Office of Drugs and Crimes (UNODC)** are as follows:

The Deep Web is defined as "a part of the World Wide Web that is not discoverable by search engines, includes password-protected information - from social networks through to email servers."[273]

The Dark Web is defined as "a collection of thousands of websites that use anonymity tools like TOR to encrypt their traffic and hide their I.P. addresses. The high level of anonymity in the digital space enables criminals to act without being easily detected."

The concept of Dark Web can be understood from the iceberg example:



[273]Global Programme on Cybercrime - United Nations Office <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>

Surface Web is the part of the World Wide Web frequently used by crores of people all over the world. It is an assemblage of indexed web pages that are administered by the most significant search engines such as Google, Bing or Yahoo, and come up as exploration results any time one types in an online search request. It comprises of a tiny part of approximately four per cent of the entire web, depending on an application and the number of the pages indexed.[274]

The Deep Web is formed by a massive amount of not indexed pages which comprises of approximately ninety per cent of the total content available on the Net and lies underneath the surface and is not observable to the search engines. It can be correlated to an iceberg which is below the water surface, hidden but massive in size and away from the eyesight. It is inclusive of government resources, legal documents, medical records, scientific reports, academic information, subscription information and even data stored on home-area networks etc. One can approach such kind of data by entering their bid into a search box of a specific site or retrieving the password-protected domain.[275]
The deep web is safe for use with precautions but not the whole part of it.

The Dark Web is a small fraction of the Deep Web which is buried at the utmost underneath section of the Net and cannot be accessed through the ordinary browsers. For such entry, one needs to use the encryption tools such as The Onion Router (hereafter called as TOR). Any user remains unidentified on TOR due to the linkage of the virtual tunnels offered by the encryption tools. There is no method to recognise anyone's physical location or trace the list of the websites one accesses, any posts or communications.
The anonymity offered by the Dark Web attracts all sorts of cyber-bullies, hackers, online fraudsters, predators, and criminals who can easily conceal their identity.

Dark Web is generally and easily misused for criminal, illegal, anti-national activities other than for useful emergency, research or meaningful purposes.

[274] Andy Greenberg, "An Interview with Darkside, Russia's Favorite Dark Web Drug Lord," Wired.com, December 4, 2014
[275] Kim Zetter, "New Service Makes Tor Anonymized Content Available to All," Wired.com, December 12, 2008

The dark web forms a small part of the Deep Web, and these terminologies are confused with a lot.

Various jurisdictions have created and implemented laws to ensure the misuse of the dark web, which will be discussed further. However, it still stands to be a part of the very dangerous resource, easily mishandled and manipulated for the crime. Since the location and I.P. address is all unidentifiable, the jurisdiction remains highly debatable and challenging to trace, causing the victim and the perpetrator to be from widely different domains.

There are two specific areas of Dark Web that cannot rationally be categorised as exclusively beneficial but have some commendable features: whistleblowing and hacktivism.

- Whistleblowing is an indispensable part of what keeps republics in check. Nonetheless, it can treacherously uncover government approaches and sources if it is not done through sanctioned channels. If these whistle-blowers use legal channels to make their grievances, the complications could have been handled without publicly broadcasting classified evidence.

- Hacktivism is another issue that ponders in a grey area. While the goals of few hacktivists may be contentious, their approaches are often offensive, and more vitally, illegal.

1.4 DANGER AND CRIMES IN DARK WEB

Broadly, cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse.It also includes online frauds, purchases of drugs online and online money laundering.Child sexual exploitation and abuse comprise abuse on the surface net or dark Net.[276]

There is no global definition of cybercrime or cyberattacks. Offences archetypally bunch around the following categories as per the United Nations Office of Drugs and Crimes (UNODC) are:

[276] Michael K Bergman, The Deep Web: Surfacing Hidden Value, Bright Planet, September 24, 2001

i) attacks against the confidentiality, integrity and availability of computer data and systems;

ii) computer-related batteries;

iii) content-related attacks

iv) offences related to infringements of copyright and related rights.

A variety of malevolent actors influence cyberspace, from criminals to terrorists to state-sponsored spies. The web can serve as a forum for discussion, harmonisation, and deed. Precisely, they may rely upon the Dark Web to assist in carrying out their activities with abridged risk of uncovering.

In this 21st century, criminals have been increasingly relying on the Internet and progressive technologies to further their criminal operations.

Bitcoin added on to the dismay of such frivolous transactions by saving up the source of the owner and helped into more of such undisclosed transactions. Bitcoin laundering services helps to intensify the anonymity of money moving through the bitcoin system. Still, eventually, most bitcoin users end up extracting the money from the scheme to be converted into cash or other types of conventional payment means.

The case of Silk Route made the dark web more popular. The much-trumpeted shutting down of the Tor-accessible illicit market known as Silk Road in 2013 October followed by the arrest of its founder Robert Ulbricht hit a blow to consumer dependability in the market for illegal goods and narcotic drugs that are made available on the Tor network. Nonetheless, this victory of for the U.S. multi-agency task force was a massive step towards bringing such illegal acts out in public and a small step towards the end of black markets hosted on the Dark Web or the availability of drugs anonymously bought online. Ross Ulbricht was a former darknet operator who created and ran the Silk Road market which is like the Amazon but dealt with drugs, arms and other illegal products and services. He was jailed in 2013 on charges of money laundering, computer hacking, and treason to traffic narcotics.[277]

[277] Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No. 6, February 2015, p 1

1.5 LAWS ACROSS DIFFERENT JURISDICTIONS

Other than the universal laws, the role of government and policymakers along with the administration is vital to regulate the dark web. The legality of the use of the dark web gets very clumsy as the reference can be made only through the cyber-crime and its close-knitted aspects. The difficulty to regulate and monitor dark web is that the jurisdiction remains unidentified. Moreover, most countries do not make the use of dark web illegal but conducting illegal activities on obscure web offence, and few with stricter laws make even the entering dark web illegal. This global battle to legalise or not legalise the use of dark web across the nations makes it much more challenging to monitor and regulate.

The United Nations General Assembly passed a resolution 65/230. It also gave the Commission on Crime Prevention and Criminal Justice resolutions 22/7, 22/8 along with the Global Programme on Cybercrime. This obliges the Member States to assist in the struggle against cyber-related crimes over competence building and technical aid.

Preceding to the instigation of the Global Programme, UNODC's had an open-ended intergovernmental professional assembly which was founded to conduct a comprehensive analysis of the delinquent of cybercrime and reactions to it by the Member States, the international community and the private sector. This effort comprises the swapping of information on national legislation, most excellent practice, technical aid and international collaboration.[278]

The United States presently has few laws that apply to Dark Web activity. Still, they were not explicitly designed to meet the challenge of the Dark Web — for example, the Dark Web easily support hacking where they can purchase virus or hacking software from other hackers, or otherwise. Now, hacking is governed by the Computer Fraud and Abuse Act (CFAA), which prevents trespassing on, proscribed accessing of, and damaging computers in interstate or international commerce. These U.S. laws are entirely sufficient to handle hacking even then, they do not accurately control the challenge of anonymity online and are not necessarily valid beyond

[278] Bright Planet, Deep Web: A Primer,
<http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/>

U.S. territorial jurisdiction, from where a maximum of the cybercrime abreast the U.S. is launched.

China has a stringent policy and bans the use of Dark web for any purpose even if it means for journalism or anything else. It forbids every entry and has made resolutions to block access to Tor.

Russia has made attempts to anonymise Tor for political objectives. Russia has recently declared some of the most stringent and most harsh laws concerning internet use and Dark Web activity - 'anti-terrorism' legislation which went into effect in 2016. Russia's Federal Security Service started enforcing the law by collecting encryption keys from internet service providers. A denial to hand over keys can charge one with a fine of approximately fifteen thousand U.S. Dollars. The Russian government is also making efforts to crack the anonymity of the Dark Web for such they are entering into research contracts with big groups.
In the European Union, once the user in Europe has acknowledged the identity, then civil charges can be lodged under the following:
Directive 2004/48/EC on the enforcement of intellectual property rights
Regulation (E.C.) No 864/2007 on the law applicable to non-contractual obligations
Regulation (E.U.) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.[279]

Austria has made attempts to eliminate Tor traffic within its borders. One of the most climactic policy actions in 2014 was when the authorities arrested a person who had made his computer a Tor relay, and held him responsible for 'contributing to the completion' of a cybercrime committed by a different Tor user who had no role to play with the arrested man, other than the fact that the cybercriminal's traffic was routed through the Austrian man's computer. This verdict of Clemmitt 2016, set a precedent that it is potentially illegal to operate a Tor exit relay in Austria, which is a significant blow to Austrians who wish to support the project.[280]

[279]The Rome II Regulation
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1314749>
[280](Ec.europa.eu, 2020)
<https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-305-EN-F1-1-ANNEX-1.PDF>

The struggle lies at the point where the U.S. and Germany supported Tor, to the extent of even funding it whereas the international community vehemently opposes it. This poses a vital challenge for global policy development. Cooperation between Austria and the U.S. would be confronting as well.[281]

Opposite to general understanding, other than in China, using proxy networks in and of itself is legal. Simply visiting Dark Web markets like Empire Market, Dream Market, and Nightmare Market is usually permissible. Mostly across the globe, one needs to conduct and illegal activity explicitly to be considered as a criminal within dark web, merely visiting or using it is not unlawful.

Catching dark web users is complicated. The location of the perpetrator remains unclear; however, advanced techniques and one silly move by the user helps in revealing the identity.
One can say that this struggle will always prevail as the international agencies do not want to ban the dark web because of its various advantages of privacy and identity security but keeping a check on it is similarly challenging and almost seems impossible in most cases. With the advent of technology, one can say that the breaking of privacy will become more comfortable. Still, the simultaneous growth in keeping it hidden will also see a similar increase.
Unfortunately, criminals can efficiently leverage the Internet to conduct conventional crimes such as dealing in illicit drugs and sex trafficking. Moreover, they employ the digital world to aid crimes that are usually technology-driven, including identification theft, payment card scam, and intellectual property fraud.
The Dark Web has been referred to as promoting a wide variety of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography.

[281]Kramer, Xandra E, The Rome II Regulation on the Law Applicable to Non-Contractual Obligations: The European Private International Law Tradition Continued - Introductory Observations, Scope, System, and General Rules (October 15, 2008). NederlandsInternationaalPrivaatrecht (NIPR), No. 4, pp. 414-424, 2008. Available at <https://ssrn.com/abstract=1314749>

In the coming future, we can hope to develop a more effective international regulation to ensure safety from such unnamed and unidentified criminals.

In present times, several institutions manage a secured website within the dark web, including press agencies, Facebook, and even government bodies because it guarantees its commitment to privacy.

1.6 LET'S SUM UP

In this chapter, we have studied the basic concepts and definitions of Dark Web for a better understanding along with the danger and crimes in Dark Web. Finally, we ended the discussion with the laws pertaining to dark web across different jurisdictions.

1.7 FURTHER READING

- Michael K. Bergman, The Deep Web: Surfacing Hidden Value, Bright Planet, September 24, 2001.
- The Internet is also used for email, file transfers, and instant messaging, among other things. Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No. 6 February 2015.
- Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No. 6 February 2015, p. 1.
- Beshiri, Arbër&Susuri, Arsim. (2019). Dark Web and Its Impact on Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications. 07. 30-43. 10.4236/jcc.2019.73004.
- Bright Planet, Deep Web: A Primer, http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **Define Deep Web?**

The Deep Web is defined as "a part of the World Wide Web that is not discoverable by search engines, includes password-protected information - from social networks through to email servers."

2) **What is the Dark Web?**

The Dark Web is defined as "a collection of thousands of websites that use anonymity tools like TOR to encrypt their traffic and hide their I.P. addresses. The high level of anonymity in the digital space enables criminals to act without being easily detected."

3) **What are crimes related to Dark Web?**

i) attacks against the confidentiality, integrity and availability of computer data and systems;
ii) computer-related batteries;
iii) content-related attacks
iv) offences related to infringements of copyright and related rights.

4) **What is the policy of China pertaining to Dark Web?**

China has a stringent policy and bans the use of Dark web for any purpose even if it means for journalism or anything else. It forbids every entry and has made resolutions to block access to Tor.

1.9 ACTIVITY

Explain the concept of Dark Web and the crimes pertaining to it along with the laws that have been enacted in varied jurisdictions? (1000 words)

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-949119-8-2

BAOU
Education for All

Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-103

Domestic Regulatory Framework

Post Graduate Diploma in Cyber Law (PGDCL)

2020

Domestic Regulatory Framework

Dr. Babasaheb Ambedkar Open University

Domestic Regulatory Framework

Course Writer

Dr.DeeshaKhaire Assistant Professor (Law), Gujarat National Law University, Gandhinagar

Content Editors

Prof. (Dr.) Nilesh K. Modi Professor & Director, School of Computer Science
Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. June 2020

This publication is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) https://creativecommons.org/licenses/by-nc-sa/4.0/

ISBN:978-81-949119-9-9

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

PGDCL-103

Domestic Regulatory Framework

Block-1: INFORMATIONAL TECHNOLOGY ACT, 2000(AMENDED IN 2008): BRIEF UNDERSTANDING

UNIT-1 JURISDICTIONAL ASPECTS OF CYBER LAW 006

UNIT-2 BEST PRACTICES OF CYBER LAW ACROSS THE WORLD 017

UNIT-3 THE APPELLATE TRIBUNAL AND LATEST AMENDMENTS 028

UNIT-4 FACETS OF CYBERCRIME: OFFENCES, PENALTIES AND COMPENSATION 037

Block-2: DIGITAL SIGNATURE, ELECTRONIC SIGNATURE AND LAWS RELATED TO CERTIFYING AUTHORITY OF INDIA

UNIT-1 DIGITAL AND ELECTRONIC SIGNATURE: CONCEPT AND PROCEDURE 054

UNIT-2 DIGITAL SIGNATURE CERTIFICATE 066

UNIT-3 REGULATION AND RESPONSIBILITIES OF CERTIFYING AUTHORITIES AND CONTROLLER OF CERTIFYING AUTHORITIES 077

UNIT-4 ADDRESSING OFFENCES: PENALTIES AND COMPENSATION 087

Block-3: LAWS RELATED TO E-SERVICE DELIVERY AND SERVICE PROVIDERS

UNIT-1E-SERVICES DELIVERY LAWS IN INDIA 100

UNIT-2RULES AND REGULATIONS RELATED TO CYBER CAFE 111

UNIT-3 RULES AND REGULATIONS RELATED TO SERVICE PROVIDER'S LIABILITY 120

UNIT-4 E-HEALTH AND REGULATORY FRAMEWORK 131

Block-4: LAWS RELATED TO DATA PROTECTION IN INDIA

UNIT-1 LAW RELATED TO SENSITIVE PERSONAL DATA IN INDIA 144

UNIT-2 LAWS RELATED TO ONLINE DEFAMATION 155

UNIT-3 BODY CORPORATE'S RESPONSIBILITIES FOR DATA PROTECTION 166

UNIT-4 RIGHT TO BE FORGOTTEN 174

Block-1
Information Technology Act, 2000 (Amended in 2008): Brief Understanding

Unit 1: Jurisdictional Aspects of Cyber Law

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Issues of Jurisdiction

1.4 Extraterritorial Jurisdiction

1.5 The 'Effects Doctrine'

1.6 Personal Jurisdiction

1.7 Tests involved to determine Jurisdiction

1.8 The Effects test and Intentional targeting

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Issues of Jurisdiction
- Territorial and Extraterritorial Jurisdiction
- Various tests involved to determine jurisdiction

1.2 INTRODUCTION

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property and subject matter. The principles of jurisdiction are

enshrined in the Constitution of a State and part of its jurisdictional sovereignty.[1] All sovereign independent States possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arising within these limits.[2]

1.3 ISSUES OF JURISDICTION

The issue of jurisdiction has been looked at from two perspectives.[3] They are:-

- ***Prescriptive Jurisdiction***

  It describes a State's ability to define its own laws in respect of any matter it chooses. A State's prescriptive jurisdiction is unlimited and a State may legislate for any matter irrespective of where it occurs or the nationality of the persons involved.

- ***Enforcement Jurisdiction***

  A State's ability to enforce laws is necessarily dependent on the existence of prescriptive jurisdiction.A State's enforcement jurisdiction within its own territory is presumptively absolute over all matters and persons situated therein. The State's legislative enactments primarily reflect its prescriptive jurisdiction.

1.4 EXTRATERRITORIAL JURISDICTION

Public International Law reflects the juxtaposition of States (as a legal person) and subjects their jurisdictional sovereignties to certain limitations, i.e., there is 'general prohibition in international law against the extraterritorial application of domestic laws.[4] The Supreme Court in ***British India Steam Navigation Co. VsShanmughavilas Cashew Industries***[5]**,** while dealing with Private International law, however made general observations as to the extent of

[1] Apart from judicial activity, a State's administrative, executive and legislative activity is also part of its jurisdictional sovereignity

[2] Lord Macmillan in Compania*NavieraVascongado v Steamship Cristina*, [1938] AC 485

[3] 'Cyberspace Jurisdiction and Courts in India' by Dr Ravishankar K Mor, Asst Prof Dept of Law,YeshwantMahavidyalaya, Wardha

[4] In the absence of municipal laws, international treaties ratified by India can be taken into account for framing guidelines in respect of enforcement of fundamental rights. (*Vishaka v State of Rajasthan*, [1997] 6 SCC 241, *Lakshmi Kant Pandey v Union of India*, AIR [1984] SC 469

[5]*British India Steam Navigation Co. v Shanmughavilas Cashew Industries* [1990] 48 ELT 481 (SC).

applicability of the statutes enacted by the Indian Parliament and opined: "In general, a statute extends territorially, unless a contrary is stated, throughout the country and will extend to the territorial waters and such places as intention to such places is shown". It was further observed that "without anything more, Indian statutes are ineffective against foreign property and foreigners outside the jurisdiction".

The sources of the extraterritorial jurisdiction are:

a) Territorial Principle

A State's territory for jurisdictional purposes extends to its land and dependent territories, airspace, ships, territorial sea and, for limited purposes to its contiguous zone, continental shelf and Exclusive Economic Zone (EEZ). The said principle as adopted by the national courts has been that all persons within a State's territory are subject to national law, save only for those granted immunity under international law.

The territorial principle has two variants:

a) 'Objective' territorial principle, where a State exercises its jurisdiction over all activities that are completed within its territory, even though some element constituting the crime or civil wrong took place elsewhere; and

b) 'Subjective' territorial principle, where a State asserts its jurisdiction over matters commencing in its territory, even though the final event may have occurred elsewhere.

In ***SS Lotus Case (France Vs Turkey),***[6]it was held by the Permanent Court of International Justice that "the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial i.e., it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".

b) Nationality Principle

It is for each State to determine under its own law who its nationals are. The nationality of a person of a particular State shall be determined in accordance with the law of that State.

[6]*SS Lotus Case (France v Turkey)*PCIJ Ser A [1927], No 9

Nationality serves above all to determine that the person upon whom it is conferred, enjoys the rights and is bound by the obligations which the law of the State in question grants to or imposes upon its nationals.[7]

c) Protective Principle

A State relies upon this principle when its national security or a matter of public interest is in the issue. A State has a right to protect itself from acts of international conspiracies and terrorism, drug trafficking, etc.

In ***Attorney-General of the Government of Israel v Eichmann,***[8]the District Court of Jerusalem held:

The State of Israel's 'right to punish' the accused derives, in our view, from two cumulative sources: a universal source (pertaining to the whole of mankind), which vests the right to prosecute and punish crimes of this order in every State within the family of nations; and a specific or national source, which gives the victim nation the right to try any who assault its existence.

d) Passive Personality Principle

It extends the nationality principle to apply to any crime committed against a national of a State, wherever that national may be. It, in a way, provides that the citizen of one country, while visiting another, takes with him for his "protection" the law of his own country and subjects the operation of that law upon those with whom he comes into contact. The passive personality principle authorizes States to assert jurisdiction over offences committed against their citizens abroad.[9]It recognized that each State has a legitimate interest in protecting the safety of its citizens when they journey outside national boundaries. Though the principle may be referred to as a controversial one, as it extends the ***'arm of national laws further even in the foreign territories'.*** Nevertheless, the principle has been adopted as a basis for asserting jurisdiction over hostage-takers.[10]

e) Universality Principle

[7]*Nottebohm Case (Liechtenstein v Guatemala*) (Second Phase), ICJ Rep [1955] 4
[8]*Attorney-General of the Government of Israel v Eichmann* 36 ILR [1961] 5
[9]*United States v Yunis*, 681 F Supp 896 [1988]
[10] See, International Convention against the taking of hostage, 1979

The canvass of the universality principle is quite vast. A State has jurisdiction to define and prescribe punishment for certain offences recognized by the community of nations as of universal concern. It includes acts of terrorism, attacks on or hijacking of aircrafts, genocide, war crimes etc. A State may assert its universal jurisdiction irrespective of who committed the act and where it occurred.

The principles of jurisdiction of international law take cognizance of both State and international laws. If on one hand the objective of the State (or municipal or domestic) law is not only to ascertain the supremacy of its judicial sovereignty domestically but also extra-territorially, then on the other the international law itself imposes general prohibition against the extraterritorial application of domestic laws.

1.5 THE EFFECTS DOCTRINE

It is an extra-territorial application of national laws where an action by a person with no territorial or national connection with a State has an effect on that State. The situation is compounded if the act is legal in the place where it was performed. The 'Effects Doctrine' is primarily a doctrine to protect American business interests and is applicable where there are restrictive trade or anti-competitive agreements between corporations. In ***Hartford Fire Insurance Co. Vs California***[11]**,** the question was whether the London Insurance Companies refusing to grant reinsurance to certain US businesses, except on terms agreed amongst themselves are violative of the US anti-trust laws and tried in the United States. The US Supreme Court held that the US Court did have jurisdiction and that there exists no conflict between domestic and foreign law and "where a person subject to regulation by two states can comply with the laws of both".

1.6 PERSONAL JURISDICTION

Personal Jurisdiction is the competence of a court to determine a case against a particular category of persons (natural as well as juridical). It requires a determination of whether or not the person is subject to the court in which the case is filed. It is classified into:-

- ***General Jurisdiction***

[11] *Hartford Fire Insurance Co. v California* 113 S Ct 2891 [1993]

The General Jurisdiction subjects a person to the power of the applicable court with respect to any cause of action that might be brought. It has historically relied on very close contacts of the person with the state, such as residency or domicile within the state, physical presence in the state at the time of service of process, etc.

- ***Specific Jurisdiction***

The Specific Jurisdiction refers to the power of the applicable court with respect to a particular cause of action based upon some set of 'minimum contacts' with the forum state that relate to that cause of action.

1.7 TESTS INVOLVED TO DETERMINE JURISDICTION

- ***Minimum Contacts Test***

In ***International Shoe Co. Vs Washington***[12]**,** a two-part test for determining the jurisdiction of the forum court over a defendant not residing or carrying on business within its jurisdiction was evolved. It was held that in such an instance, the plaintiff would have to show that the defendant has sufficient'minimum contacts' in the forum state. In other words, the defendant must have purposefullydirected its activities towards the forum state or otherwise 'purposefully availed' of the privilege of conducting activities in the forum state. Further, the forum court had to be satisfied that exercising jurisdiction would comport with the traditional notions of fair play and substantial justice. The minimum contacts test in the said case has been understood as to have performed "two related, but distinguishable, functions."[13] The first was to protect the defendant from the burden of litigating in a distant or inconvenient forum.[14] The second was to ensure that the states do not "reach out beyond the limits imposed on them by their status as coequal sovereigns in a federal system."[15]

- ***Purposeful Availment Test***

In ***Burger King Corp VsRudzewicz***[16]**,** the Supreme Court held that the defendant did not have to be physically present within the jurisdiction of the forum court and that the forum court may exercisejurisdiction over a non-resident where an alleged injury arises out of or

[12]*International Shoe Co v Washington* 326 U S 340 [1945]
[13]*World-Wide Volkswagen v Woodson*, 444 U.S. 286, 291-92 [1980]
[14] Id
[15] Supra note 12
[16]*Burger King Corp v Rudzewicz*471 U S 462 [1985]

relates to actions by the defendant himself that are 'purposefully directed' towards residents of the forum state. It was held that **'purposeful availment'** would not result from 'random' or 'fortuitous' contacts by the defendant in the forum state. It requires the plaintiff to show that such contracts resulted from the "actions by the defendant himself that created a substantial connection with the forum state." He must have engaged in 'significant activities' within the forum state or created 'continuing obligations' between himself and the residents of the forum state. It was held on facts, the twenty-year relationship that the defendant had with the plaintiff "reinforced his deliberate affiliation with the forum state and the reasonable foreseeability of litigation there."

In ***Ballard v. Savage***[17]**,**it was explained that the expression 'purposefully availed' meant that "thedefendant has taken deliberate action within the forum state or if he has created continuing
obligations to forum residents." It was further explained that "it was not required that a defendant be physically present within, or have physical contacts with the forum, provided that hisefforts are purposefully directed toward forum residents."

In ***CompuServe, Inc. v. Patterson***[18]**,** it was found that the defendant had chosen to transmit its products from Texas to CompuServe's system and that the system provided access to his software to others to whom he had advertised and sold his product. It was held that Patterson had "purposefully availed himself of the privilege of doing business."

- ***Sliding Scale Test***

An extension of the purposeful availment test was attempted in ***Zippo Mfg. Co. v. Zippo Dot Com,Inc.***[19]The issue of specific personal jurisdiction arose in the context of trademark dilution, infringement and false designation under the Federal Trademark Act. The court in ***Zippo***classified websites as passive, interactive and integral to the defendant's business. It was held that "At one end of the spectrum are situations where a defendant clearly does businessover the Internet. If the defendant enters into contracts with residents of a foreignjurisdiction that involves the knowing and repeated transmission of computer

[17]*Ballard v Savage*65 F3d 1495 (9th Cir) [1995]
[18]*CompuServe, Inc v Patterson*89 F 3d 1257 (6th Cir) [1996]
[19]*Zippo Mfg Co v Zippo Dot Com,Inc*952 F Supp 1119 (W D Pa) [1997]

filesover the Internet, personal jurisdiction is proper. At the opposite end are situationswhere a defendant has simply posted information on an Internet Website, which isaccessible to users in foreign jurisdictions. A passive Website that does little morethan make information available to those who are interested in it is not grounds forthe exercise of personal jurisdiction. The middle ground is occupied by interactiveWebsites where a user can exchange information with the host computer. In thesecases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Website".

In ***Millennium Enterprises Inc. v. Millennium Music L.P.***[20] the Oregon district court declined toexercise jurisdiction over a South Carolina corporation that sold products both offline and on the web. The court felt that ***'something more'*** than merely showing that the website was interactive was required. The defendant should be shown to have consummated some transaction within Oregon and to have made 'deliberate and repeated contacts' with Oregon through the website so that it could be held that they ought to have anticipated being hauled into an Oregon court.

1.8 THE EFFECTS TEST AND INTENTIONAL TARGETING

The difficulty experienced with the application of the ***Zippo sliding scale test*** has paved the way for the application of the 'effects' test. The courts have thus moved from a 'subjective territoriality' test[21]to an 'objective territoriality' or 'effects' test in which the forum court will exercise jurisdiction if itis shown that effects of the defendant's website are felt in the forum state. In other words, it musthave resulted in some harm or injury to the plaintiff within the territory of the forum state. Sincesome effect of a website is bound to be felt in several jurisdictions given the nature of the internet,courts have adopted a 'tighter' version of the 'effects' test, which is 'intentional targeting.'

[20]*Millennium Enterprises Inc v Millennium Music L P*33 F Supp 2d 907 (D Or) [1999]

[21] That a court will regulate an activity only if it is shown having originated in its territory – exemplified by the decisionin *Louis Feraud Int'l SARL v Viewfinder Inc*,406 F Supp 2d 274 (S D N Y) [2005]

The 'effects' test was first evolved in ***Calder v. Jones.***[22]In the said case, the Court held that a California court could assert jurisdiction over a Florida publisher that published an article defaming the plaintiff, in view of the facts that the plaintiff resided in California. The Court reasoned that the defendants had engaged in "intentional, and allegedly tortious, actions that were expressly aimed at California", and that "they knew that the brunt of the injury would be felt" by the plaintiff in California.

The 'Effects Test' is a further extension of the 'forum state targeting', as it also takes into consideration the effect that "out-of-state" conduct has in the forum state. Thus, in order to have personal jurisdiction, there must be:-

- Intentional actions
- Expressly aimed at the forum state
- Causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state.

1.9 LET'S SUM UP

In this chapter, we have studied the issues of jurisdiction along with extraterritorial and personal jurisdiction. We also studied the tests involved in determining jurisdiction. Finally, we ended the discussion with the Effects Test and Intentional targeting.

1.10 FURTHER READING

- Brenner, Susan. (2004). Cybercrime jurisdiction. J. High Tech. L. 1. 10.1007/s10611-007-9063-7.
- Brenner, Susan &Koops, Bert-Jaap. (2005). Approaches to Cybercrime Jurisdiction. Journal of High Technology Law. 4.
- Egyankosh.ac.in (2019), http://egyankosh.ac.in/bitstream/123456789/7634/1/Unit-10.pdf (last visited Nov 27, 2019).

[22]*Calder v Jones*465 U S 783 [1984]

- AmitaVerma, Cyber Crimes and Law, Central Law Publications, Allahabad, 2009, p.318.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the issues of jurisdiction associated with cyber laws?

The issues of jurisdiction associated with cyber laws are as follows:

- *Prescriptive Jurisdiction* - It describes a State's ability to define its own laws in respect of any matter it chooses. A State's prescriptive jurisdiction is unlimited and a State may legislate for any matter irrespective of where it occurs or the nationality of the persons involved.
- *Enforcement Jurisdiction* – It deals with a State's ability to enforce laws is necessarily dependent on the existence of prescriptive jurisdiction.A State's enforcement jurisdiction within its own territory is presumptively absolute over all matters and persons situated therein. The State's legislative enactments primarily reflect its prescriptive jurisdiction.

2. What are the principles associated with extra-territorial jurisdiction vis-à-vis cyber laws?

The principles associated with extra-territorial jurisdiction vis-à-vis cyber laws are as follows:-

- Territorial principle
- Nationality Principle
- Protective Principle
- Passive Personality Principle
- Universality principle

3. What is meant by the 'Effects Doctrine'?

The Effects Doctrine is an extra-territorial application of national laws where an action by a person with no territorial or national connection with a State has an effect on that State.

4. What are the tests involved in determining jurisdiction?

The tests involved in determining jurisdiction in instances involving disputes of cyber laws are as follows:

- Minimum Contacts Test

- Purposeful availment Test

- Sliding Scale Test

5. What is understood by 'personal jurisdiction' in context of cyberspace?

Personal Jurisdiction is the competence of a court to determine a case against a particular category of persons (natural as well as juridical) involving a dispute arisen associating with cyberspace. This can comprise of either general jurisdiction or specific jurisdiction.

1.12 ACTIVITY

"The effectiveness of any judicial system rest on the bedrock of jurisdiction itself'.Explain the jurisdiction issues in Internet-based on US law as well as Indian law. (2000-2500 words)

Unit 2: Best Practices of Cyber Law across the World

2

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 USA
1.4 UK
1.5 Canada
1.6 Suggestions derived from Best Practices across the world
1.7 Let's sum up
1.8 Further reading
1.9 Check your progress: Possible answers
1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- How cyber law is being implemented in the countries - USA, UK, Canada and Australia
- The policies and laws which are effective in creating and maintaining a safe cyber space.
- The policies and laws which are the best practices and can be inculcated in our country for reference.

1.2 INTRODUCTION

There are more than 7 billion people in this world with almost 50% on as an internet user. This number keeps on increasing exponentially, every single day. This generation can be called the internet generation and the century being the internet century. For a while we can imagine our lives without food or water but surviving without internet for hours seems impossible. Today we connect with our family, friends, peers and everyone else in the world through the internet

creating and implementing in true sense the idea of a global village without borders. World connectivity has brought about such a revolution that the post-net and pre-net worlds are entirely unrecognizable. With the increasing popularity of online activities, the rate of online crimes has also increased exponentially. While the extent and impact of these crimes vary greatly across the globe but in totality it has become a universal nuisance. From cyber bullying to cyber terrorism, newer technology is providing fertile lands for newer crimes.[23]

Understanding and having knowledge about the cyber law of various countries is extremely crucial because cyber space is not restricted to the territorial understanding of a state, rather is spread across the globe without much demarcations. It touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. cyber activities are not governed by geographical borders, which makes dealing with such crimes all the more confusing and complex and therefore, a lot of cyber-crimes go unreported. Apart from the International law and guidelines in this field, it is also important to understand how the other jurisdictions work in order to check this invisible vast omnipresent space.[24]

1.3 USA

The United States have been a prime sufferer of cyber-crime in the world. However, it has devised a very strong cyber law in place and keeps working and updating that with the very speed of technology transformation. Around sixty percent of cyber cries are filed in the USA have been convicted and sentenced. The cyber laws and privacy system of the States is arguably the oldest, most robust and effective in the world.

The Computer Fraud and Abuse Act of 1986 (CFAA), enacted into law today as United States Code Title 18 Section 1030 (18 U.S.C. §), is the primary federal law governing cybercrime in the United States. n the 1970s and early '80s, many phone phreaks and early computer hackers ran rampant through online systems unhampered by worries of legal complications. CFAA was

[23]Cyber Laws: What Have Different Countries Done <https://unbumf.com/cyber-laws-what-have-different-countries-done-to-prevent-cyber-crime/>

[24]Miguel Mendoza and Miguel Mendoza, 'Challenges And Implications Of Cybersecurity Legislation | Welivesecurity' (*WeLiveSecurity*, 2020) <https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/>

aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.[25]

It criminalised spreading of malevolent code, trading in passwords or other access control mechanisms etc. The act defines a category of "protected computer" to exclude and safeguard the federal interest but in theory and through princely elucidation all the computers are covered.

The Act has been amended over the years to refine the definitions and to expand coverage into other aspects of cybercrime. Between 1988 and 2008, the law was amended 9 folds. A lot of updates included mounting security to financial institutions and other private computers, including civil actions, adding tampering and attempted extortion, criminalising of taking information off of systems etc.[26]

The important provisions under this law are:

S. No.	Section Number	Act - The Computer Fraud and Abuse Act of 1986 (CFAA)
1	**1028**	**Fraud and related activity in connection with identification documents, authentication features, and information**
2	**1028A**	**Aggravated identity theft**
3	**1029**	**Fraud and related activity in connection with access devices**
4	**1030**	**Fraud and related activity in connection with computers**
5	**1037**	**Fraud and related activity in connection with electronic mail**
6	**1343**	**Fraud by wire, radio, or television**
7	**1362**	**Malicious mischief related to communications lines, stations, or systems**

[25]Kamble, R (2013). CYBER LAW AND INFORMATION TECHNOLOGY.International Journal of Scientific and Engineering Research. 4. 789-794

[26]Eichensehr, Kristen, The Cyber-Law of Nations (January 8, 2014) 103 Geo L J 317 (2015)

8	**1462**	**Importation or transportation of obscene matters**
9	**1465**	**Transportation of obscene matters for sale or distribution**
10	**1466A**	**Obscene visual representation of the sexual abuse of children**
11	**2251**	**Sexual exploitation of children**
12	**2252**	**Certain activities relating to material involving the sexual exploitation of minors**
13	**2252A**	**Certain activities relating to material constituting or containing child pornography**
14	**2252B**	**Misleading domain names on the Internet [to deceive minors**
15	**2252C**	**18 U.S.C. §– Misleading words or digital images on the Internet**
16	**2425**	**Use of interstate facilities to transmit information about a minor**
17	**2319**	**Criminal infringement of a copyright**
18	**2510-2522**	**Interception of wire, oral, or electronic communication**
19	**2701-2712**	**Preservation and disclosure of stored wire and electronic communication**
20	**3121-3127**	**Pen registers and trap and trace devices**

The Electronic Communications Privacy Act, 1986 allows the government to access digital communications such as email, social media messages, information on public cloud databases, and more with a summon. No warrant is required if the items in question are 180 days old or older.

Cyber Intelligence Sharing and Protection Act (CISPA), 2011 was reintroduced in 2015 at the Parliament as an amendment to the National Security Act of 1947. This was set up with the objective of improving cybersecurity by sharing information on potential cyber threats with the federal government.

Children's Online Privacy Protection Act (COPPA), 2012 was implemented in 2013 which mandated websites that gather data on children under the age of thirteen to conform with the Federal Trade Commission (FTC), which governs whether a website is suitable for children by reviewing its language, content, advertising, graphics and features, and intended audience.

It can be concluded that US has some pretty high levels of security when it comes to cyber safety and the cyber laws are much varied and comprehensive. the government has been working to introduce stricter laws to equip organizations to secure the data from the latest cyber threats. In conclusion one can say that USA does set a good example for cyber laws and security across the world.[27]

In the year 2014, these new legislations were introduced:

S. No.	Legislation
1	**National Cybersecurity Protection Act (NCPA)**
1	**Cybersecurity Enhancement Act of 2014 (CEA)**
2	**Federal Information System Modernization Act of 2014 (FISMA 2014)**
3	**Cybersecurity Workforce Assessment Act (CWWA)**
4	**Border Patrol Agent Pay Reform Act (BPAPRA)**

1.4 UK

The United Kingdom has been fighting issues of cyber-crime and cyber security over a lot of years. Most recently the case of ***'Cambridge Analytica'*** also dwelled around the Data Protection laws and brought about a new regulation for the European Union. In UK, there is a demarcation between two types of cyber- crimes. They differentiate between a cyber-enabled crime and a cyber-centric crime. Cyber-centric crimes are things like unauthorised access to computer systems, new crimes brought about through the existence of computers. However, cyber-enabled

[27] WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009), available at <http://www.whitehouse.gov/assets/ documents/Cyberspace_Policy_Review_final.pdf>

crimes are crimes that have always existed, but benefit from the existence of computers such as fraud.[28]

The list of significant legislations specifically for cyber-crimes is:[29]

S. No.	Legislation	Purpose
1.	**Malicious Communications Act 1988**	**It dealt with communication and its malice and offense caused**
2.	**Official Secrets Act 1989**	**It deals with national security**
3.	**Computer Misuse Act 1990**	**It specifies various hacking offences**
4.	**Data Protection Act 1998**	**It implements the Data Protection Directive 1995**
5.	**Communications Act 2003**	**It is the main source of UK telecommunications law**
6.	**Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)**	**It regulated the communication and data protection for electronic communication.**
7.	**Serious Crime Act 2015**	**It defines principles for the protection of data**

The Computer Misuse Act, 1990 (CMA) is the chief piece of UK legislation relating to offences or attacks against computer systems such as hacking or denial of service. The act left space for technological advancement and did not define a 'computer'. In ***DPP v McKeown and, DPP v Jones [1997] 2 Cr App R 155 HL,*** Lord Hoffman defined computer as 'a device for storing, processing and retrieving information'; this means that a mobile smartphone or personal tablet device could also be defined as a computer in the same way as a traditional 'desk-top' computer or 'PC'. There is jurisdiction to prosecute all CMA offences if there is "at least one significant link with the domestic jurisdiction" (England and Wales) in the circumstances of the case."

[28] GOV'T OF KENYA, CYBERSECURITY STRATEGY 12 (2014), available at <http://www.icta.go.ke/wpcontent/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf>

[29] U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 11 (2011), available at <https://www.gov.uk/government/publications/cyber-securitystrategy>

Offences under the Computer Misuse Act are tabled below:

S. No.	Section Number	Act - The Computer Misuse Act, 1990 (CMA)
1	**1**	**Unauthorised access to computer material, it involves 'access without right' along with an intention for such**
5	**2**	**Unauthorised access with intent to commit or facilitate commission of further offences**
6	**3**	**Unauthorised acts with intent to impair the operation of a computer**
7	**3ZA**	**Unauthorised acts which tend to attack the critical national infrastructure**
8	**3A**	**It deals with those who make or supply malware.**

This act has been amended twice, by the Police and Justice Act 2006 and by the Serious Crime Act 2015.

Data Protection Act 1998 creates criminal offences that may be committed alongside cyber-dependent crimes inclusive of procuring or revealing personal data, disclosure of personal data, entailing private data for selling or offering to sell it etc.

Communications Act, 2003magnifies our understanding of our ambit of malicious and offensive communication. It also includes that when one sends through a 'public electronic communications network' a message or other matter that is 'grossly offensive' or of an 'indecent, obscene or menacing character', it is an offence. To send or false message 'for the purpose of causing annoyance, inconvenience or needless anxiety to another' is also an offence. It involves the acts of cyber bullying, cyber trolling, virtual mobbing etc.[30]

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

[30] C Matthew, Waxman Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J INT'L L, volume 421, p 431 – 468 Posted: 2011

Certain other laws relating to this field in this particular jurisdiction are Police and Justice Act 2006, EU Directive 2013/40/EU, Terrorism Act 2000, Regulation of Investigatory Powers Act 2000, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Human Rights Act 1998, Extradition Act 2003, Crime and Courts Act 2013, Telecommunications (Data Protection and Privacy) Regulations 1999 etc.

UK is working towards betterment of cyber security and data protection each day. Presently on May 2018 the General Data Protection Regulation 2016/679 (GDPR) became directly effective in the UK and the Network and Information Security Directive 2016/1148 to be implemented in all member states of the European Union. But Brexit puts everything under much speculation and uncertainty.

1.5 CANADA

Canadian cyber laws are generally principles-based which provides organisations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.[31]

There are many legislations and regulations for such including Cybersecurity Best Practices Guide and a Cyber Incident Management Planning Guide 2015 launched by the Investment Industry Regulatory Organization, the Bulletin on Cybersecurity 2016 by Mutual Fund Dealers Association of Canada, Security Self-Assessment Tool by the Office of the Privacy Commissioner of Canada etc.[32]

Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) applies to the private sector to protect personal information within their possession or control. It contains implicit or explicit accountability and security obligations for personal information by federally-regulated organizations. PIPEDA was amended in 2015 was amended to ensure that any breach be reported to Office of the Privacy Commissioner of Canada. Also, the breaches have to be

[31] Eloise F Malone & Michael J Malone, "The 'wicked problem' of cybersecurity policy: analysis of United States and Canadian policy response" (2013) 19:2 Can Foreign Policy J 158 at 171

[32] Greg Weston "Foreign hackers attack Canadian Government", CBC News (16 February 2011), online: [perma.cc/Y4D3-QHLB]

reported and maintained. Knowledge of such crime and failing to report is also an offence under the act.

Bill C-59 Act, 2017 was introduced to enlarge the authorization of the Communications Securities Establishment (CSE). The act allowed the CSE authorities to interfere with foreign online efforts that threaten the country by shielding Canada's networks from foreign cyber threats – both defensively and actively. It would include degrading, disrupting, influencing, responding to or interfering with the capabilities, intentions or activities of a foreign actor.[33]

Canada has created the ***National Cyber Security Strategy*** ***and a National Cybercrime Coordination Unit,*** which coordinates for cyber-crime investigations in the country and partners internationally. They also provide digital investigative advice to Canadian law enforcement; and establish a national reporting mechanism for Canadian citizens and businesses to report cybercrime incidents. Moreover, the Canadian Anti-Fraud Centre mitigates public marketing fraud.

In the year 2012, the Ontario Court of Appeal acknowledged "intrusion upon seclusion", as tort in which "one who intentionally or recklessly intrudes, physically or otherwise, upon the seclusion of another or his or her private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person".

In the year 2016, the Ontario Court of Appeal acknowledged another privacy-related tort in ***Jane Doe 464533 v ND,*** in which, "one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."

Therefore, in Canada apart from considering cyber-crimes as criminal offence, through introducing such torts, the court adopted it as a civil offence too. It helped to establish that with the speeding technology, the need for recognition and laws to move equally fast is significant. Lawsuits involving data breaches also include more traditional allegations, such as claims of negligence, breach of contract and statutory breach.

[33] Public Safety Canada, National Cyber Security Strategy, (Ottawa: Public Safety Canada, 2018), online (pdf): [perma.cc/23W4-5MER] at 2

1.6 SUGGESTIONS DERIVED FROM BEST PRACTICES ACROSS THE WORLD

There is so much to learn from the various countries and practices about safeguarding our nation from cyber-crime and cyber terrorism. To help one understand, here are a few suggestions which can be implemented in India for a betterment in the cyber security world.

1. A tiered cybersecurity policy can be drafted. The written policy will act as a formal guide to all cybersecurity measures used in an organisation. It helps keep everyone on the loop and create a workflow which can be monitored and maintained ensuring that the levels of cyber security are maintained at every level and thereby in the entire organisation and consequently country.
2. Regulating and keeping a backup of data and maintaining a record of all the data is equally important to ensure that the data remains safe, unaltered and non-destroyable. Through regulations it must be ensured that this backed up data is thoroughly protected, encrypted and frequently updated. It is also imperative to divide backup duty among several people to mitigate insider threats.[34]
3. Partnership with other countries helps a lot in dealing with cyber-crimes as the boundary does not restrict such kind of security issues. If a country can partner with other countries and develop a system within themselves to ensure cyber security and protection against cyber-attacks, it will be way more fruitful than processing it individually.
4. Mass awareness to ensure that cyber-security is understood, dealt and tackled individually by each person is extremely crucial to ensure safety from cyber-crimes. Regulation for such can be drafted and trainings at large for public be done to ensure, everyone understand and follows those regulations can help a country at large.[35]

1.7 LET'S SUM UP

In this chapter, we have studied how cyber law is being implemented in countries like USA, UK and Canada. We also studied about the policies and laws which are effective in creating and

[34]Cyberbullying and the Law | MediaSmarts
<https://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/cyberbullying-law>
[35]Remarks by Director David Vigneault at the Economic Club
https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html

maintaining a safe cyberspace. Finally, we ended out discussion with the best practices that can be inculcated in our country.

1.8 FURTHER READING

- Singh, Umrav. (2016). Cyber Laws in India.
- Cyber Laws of Different Countries - Cyberlaws.Net, Cyberlaws.Net (2019), http://cyberlaws.net/cyber-law-repository/cyber-laws-different-countries/ (last visited Nov 24, 2019).
- Cis-india.org (2019), https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf (last visited Nov 24, 2019).
- (2019), https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=10766&context=theses (last visited Nov 24, 2019).

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is objective of the Computer Fraud and abuse Act, 1986?**

CFAA was aimed at criminal offences and did not cover civil offences by then. It offered a powerful set of prosecutorial tools to address criminal uses of computer.

2. **What does Canadian cyber laws mainly focus on?**

Canadian cyber laws are generally principles-based which provides organizations more tractability whilst covering the possible crimes. Canadian approach to Cyber Security is much more comprehensive with a lot of regulations being the responsibility of government agencies as well as private sectors.

3. **Why was Serious Crimes Act, 2015 introduced?**

Serious Crime Act 2015 covers processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. For monitoring and recording of communications in transit an artificial person must consider the act.

1.10 ACTIVITY

Elucidate the different laws and policies introduced by other countries and how it can be implemented in India along with a reason? (1000 – 1500 words)

Unit 3: The Appellate Tribunal and Latest Amendments

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Establishment of Cyber Appellate Tribunal

1.4 Latest Amendments

1.5 Overview of Telecom Disputes Settlement and Appellate Tribunal

1.6 Introduction to Telecom Disputes Settlement and Appellate Tribunal

1.7 Formation of TDSAT

1.8 Composition of TDSAT

1.9 Powers and Jurisdiction

1.10 Procedure

1.11 Nature of Proceedings

1.12 Appeals

1.13 Let's sum up

1.14 Further reading

1.15 Check your progress: Possible answers

1.16 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Establishment of Appellate Tribunal
- Latest Amendments
- Overview of Telecom Regulatory Authority of India

1.2 INTRODUCTION

Cyber Appellate Tribunal was established under the Information Technology Act, 2000 under the aegis of Controller of Certifying Authorities (CCA). It was a ***'multi-member body'.*** The Tribunal has the statutory authority to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Act. The new amendments have made the Tribunal an ***'expert body'***consisting of members having varied qualifications to appreciate the legal, technical and factual questions involved in the appeals in the first appellate stage itself.[36]

1.3 ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL

The InformationTechnology Act of India, which regulates several important aspects of electronic information, including the regulation of privateelectronic transactions as well as detailing civil and criminaloffences relating to computers and electronic information, contemplates a specialized dispute resolution mechanism for disputesrelating to the offences detailed under the Act. The Act provides forthe establishment of quasi-judicial bodies, namely adjudicatingofficers under ***Section 46,*** to hear disputes namely, offences of a civil nature under ***Section 43, 43A, 44 and 45 of the Act,*** as well ascriminal offences. The adjudicating officer has the power to bothaward compensation as damages in a civil remedy, as well as imposepenalties for the contravention of the Act, and therefore has powers of both civil and criminal courts. The first appellate body provided inthe Act, i.e. the authority that any party not satisfied by the decisionof the adjudicating officer can appeal to, is the Cyber AppellateTribunal, consisting of a Chairperson and any other members soprescribed by the Central Government. The second appeal, if a partyis aggrieved by the decision of the Cyber Appellate Tribunal, may befiled before the High Court having jurisdiction, within 60 days fromthe date of communication of the order. The proper functioning of theCyber Appellate Tribunal is particularly necessary for thefunctioning of a just judicial system in light of the provisions of theInformation Technology Act.

[36]Cyber Appellate Tribunal and its powers – Unit 6 – MyBSCIT.com <https://www.mybscit.com/cyber-law/cyber-appellate-tribunal-and-its-powers-unit-6>

As per ***Section 48 of the Act,*** the Central Government provides for an appointment of one or more appellate tribunals but the language of the ***Rule 13 of the Cyber Regulations Tribunal (Procedure) Rules, 2000*** makes it clear that there shall only be one tribunal and it shall ordinarily hold its sittings at New Delhi.[37] The said rule has further provided a lot of flexibility to Cyber Appellate Tribunal as far as its sittings are concerned. It is for the Chairperson to exercise this ***'rule of sittings'*** in a most appropriate and judicious manner. The Tribunal shall notify to the parties the date and the place of hearing of the application ***(Rule 12).*** Initially, the Tribunal consisted of only one person who was referred to as the Presiding Officer and was to be appointed by way of notification by the Central Government.[38]

It is for the Central Government to specify by order the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction. It was held by the Supreme Court in ***Union of India v Paras Laminates (P) Ltd.,***[39] "There is no doubt that the Tribunal functions as a court within the limits of its jurisdiction. It has all the powers conferred expressly by the statute. Furthermore, being a judicial body, it has all those incidental and ancillary powers which are necessary to make fully effective the express grant of statutory powers". The powers of the Tribunal are no doubt limited. Its area of jurisdiction is clearly defined, but within the bounds of its jurisdiction, it has all the powers expressly and impliedly granted.

1.4 LATEST AMENDMENTS

For the smooth functioning of any law, such law must be just,fair and reasonable and at the same time there must be aproper forum to regulate it. To give effect to the Information Technology Law, theparliament has established the most important authoritiesunder the same Act for smooth functioning. It has been rightly said by Aristotle that ***"It is better for a city to be governed by a good man than even by good laws".***

[37]THE CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE) RULES <https://law.cyberpandit.org/rule02/>
[38]A Review of the Functioning of the Cyber Appellate Tribunal <https://cis-india.org/internet-governance/blog/review-of-functioning-of-cyber-appellate-tribunal-and-adjudicatory-officers-under-it-act>
[39]*Union of India v Paras Laminates (P) Ltd*, [1990] 4 SCC 453

The Finance Act, 2017 has made several structural changes including the merging of eight powerful and autonomous administrative tribunals with other tribunals. The Government of India has moved an amendment which it proposed that the Cyber Appellate Tribunal constituted under Section 48 of the IT Act would be merged with ***Telecom Disputes Settlement & Appellate Tribunal (TDSAT)*** constituted under Section 14 of the Telecom Regulatory Authority of India (TRAI) Act.[40]

The Cyber Appellate Tribunal has not been functioning since June 2011. The jurisdiction of TDSAT extends to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. With respect to cyber matters the Tribunal exercises only the appellate jurisdiction.

The TDSAT consists of a Chairperson and two members appointed by the Central Government. Section 14C of the Act discusses about the Qualifications for appointment of Chairperson and Members.

1.5 OVERVIEW OF TELECOM DISPUTES SETTLEMENT AND APPELLATE TRIBUNAL

Telecom Regulatory Authority of India (TRAI) was enacted in 1997. TRAI is empowered to adjudicate upon disputes among service providers or between the service providers and a group of Consumers on matters relating to technical compatibility and interconnection between the Service Providers, revenue sharing arrangement between Service Providers and quality of telecommunication services and interests of consumers. TRAI was vested with the power to issue directions to the Service Providers. Appeals from the decisions of TRAI lay to the High Court and appeals therefrom lay to the Supreme Court. The jurisdiction of civil courts was barred.

In respect of Telecom, Broadcasting and Airport tariff matters, the Tribunal's orders can be appealed to the Supreme Court but only on substantial questions of law. However, no appeal lies against an interlocutory order or against any decision or order made by the Tribunal with the

[40]Probity in Governance in India
<http://www.legalserviceindia.com/articles/nkdev.htm>

consent of the parties. In regard to Cyber matters, the Tribunal's order can be appealed before High Court.[41]

1.6 INTRODUCTION TO TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL (TDSAT)

The Telecom Regulatory Authority of India Act, 1997 was amended by the Telecom Regulatory Authority of India (Amendment) Act, 2000. The amendments were introduced to resolve the issues that -emerged from the implementation of the Act. The desired objectives of bringing about functional clarity, strengthening the regulatory framework and the disputes settlement mechanism were attained by bringing about a clear distinction between the recommendatory and regulatory functions of the Telecom Regulatory Authority of India (TRAI) by making it mandatory for the Government to seek recommendations of TRAI in respect of specified matters and by the setting up a separate dispute settlement mechanism etc. An Appellate Tribunal known as the "Telecom Disputes Settlement & Appellate Tribunal" has been set up under Section 14 of the Telecom Regulatory Authority of India Act, 1997 as amended by TRAI (Amendment) Act, 2000 to adjudicate disputes and dispose of appeals with a view to protect the interests of service providers and consumers of the telecom sector and to promote and ensure orderly growth of the telecom sector. The Appellate Tribunal came into existence on 29 May 2000 and started hearing cases from January 2001.

The functions of the appellate tribunal are to adjudicate any dispute between a licensor and a licensee, between two or more service providers, between a service provider and a group of consumers, and to hear and dispose of appeals against any decision or order of TRAI, DoT and MIB. The appellate tribunal consists of a Chairperson and two Members.

1.7 FORMATION OF TDSAT

In order to bring in functional clarity and strengthen the regulatory framework and the disputes settlement mechanism in the telecommunication sector, the TRAI Act of 1997 was amended in the year 2000 and TDSAT was set up to adjudicate disputes and dispose of appeals with a view

[41]Current based PRELIMS QUESTION 19 MARCH 2020 | The Core IAS <https://thecoreias.com/current-based-prelims-question-19-march-2020/>

to protect the interests of service providers and consumers of the telecom sector and to promote and ensure orderly growth of the telecom sector. In January 2004, the Government included broadcasting and cable services also within the purview of TRAI Act. After coming into force of the relevant provisions of the Finance Act 2017, the jurisdiction of TDSAT stands extended to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal.

1.8 COMPOSITION OF TDSAT

The Tribunal consists of a Chairperson and two Members appointed by the Central Government. The Chairperson should be or should have been a Judge of the Supreme Court or the Chief Justice of a High Court. A Member should have held the post of Secretary to the Government of India or any equivalent post in the Central Government or the State Government for a period of not less than two years or a person who is well versed in the field of technology, telecommunication, industry, commerce or administration.[42]

1.9 POWERS AND JURISDICTION

The Tribunal exercises jurisdiction over Telecom, Broadcasting, IT and Airport tariff matters under the TRAI Act, 1997 (as amended), the Information Technology Act, 2008 and the Airport Economic Regulatory Authority of India Act, 2008. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. In regard to Cyber matters the Tribunal exercises only the appellate jurisdiction.

1.10 PROCEDURE

- The Tribunal is not bound by the procedure laid down by the Code of Civil Procedure, 1908;
- It has the power to regulate its own procedure;
- It is to be guided by the principles of natural justice;

[42]Telecom Disputes Settlement & Appellate Tribunal (TDSAT) <https://www.insightsonindia.com/2018/12/14/telecom-disputes-settlement-appellate-tribunal-tdsat/>

Tribunal has the same powers as are vested in a civil court under the CPC in respect of:

a) summoning and enforcing the attendance of any person and examining him on oath;
b) requiring the discovery and production of documents;
c) receiving evidence on affidavits;
d) subject to the provisions of sections 123 and 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office;
e) issuing commissions for the examination of witnesses or documents;
f) reviewing its decisions;
g) dismissing an application for default or deciding it ex parte;
h) setting aside any order of dismissal or any application for default or any order passed by it ex parte; and
i) any other matter which may be prescribed.

In addition, the Tribunal can call for the records relevant to disposing of a Petition or appeal, for the purpose of examining the legality or propriety or correctness of any decision or of any order etc. of TRAI.

1.11 NATURE OF PROCEEDINGS

- The Tribunal is the Court of first instance except cyber matters.
- Every proceeding before the Tribunal is deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196, of the Indian Penal Code (45 of 1860);
- The Tribunal is deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).
- Tribunal’s Orders are executable as a decree of civil court.

1.12 Appeals

In respect of Telecom, Broadcasting and Airport tariff matters, the Tribunal's orders can be appealed to the Supreme Court but only on substantial questions of law. However, no appeal lies

against an interlocutory order or against any decision or order made by the Tribunal with the consent of the parties. In regard to Cyber matters, the Tribunal's order can be appealed before High Court.

1.13 LET'S SUM UP

In this chapter, we have studied the concept of Cyber Appellate Tribunal along with its establishment and procedure and powers. Furthermore, we also studied when a matter can be appealed to Cyber Appellate Tribunal. Finally, we ended our discussion the latest amendments that took place in appellate tribunal and also the overview of Telecom Disputes Settlements and Appellate Tribunal.

1.14 FURTHER READING

- Krishisanskriti.org (2019), https://www.krishisanskriti.org/vol_image/22Oct2015061009zzzzzzzzzzzzzzzzzzLOVE%20KUMAR%20GUPTA%20%20%20%20%20%20%20%20%20120-122.pdf (last visited Nov 22, 2019).
- A Review of the Functioning of the Cyber Appellate Tribunal and Adjudicatory Officers under the IT Act — The Centre for Internet and Society, Cis-india.org (2019), https://cis-india.org/internet-governance/blog/review-of-functioning-of-cyber-appellate-tribunal-and-adjudicatory-officers-under-it-act (last visited Nov 22, 2019).
- http://www.tdsat.gov.in/admin/introduction/uploads/TDSAT%20INTRO.pdf

1.15 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the cyber appellate tribunal?**

Cyber Appellate Tribunal was established under the Information Technology Act, 2000 under the aegis of Controller of Certifying Authorities (CCA). It is a *'multi-member body' having* the statutory authority to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Act.

2. When was TRAI enacted?

Telecom Regulatory Authority of India (TRAI) was enacted in 1997.

3. What is the Composition of TDSAT?

The Tribunal consists of a Chairperson and two Members appointed by the Central Government.

4. What was the latest amendments that took place in the Cyber Appellate Tribunal?

The Finance Act, 2017 has made several structural changes including the merging of eight powerful and autonomous administrative tribunals with other tribunals. The Government of India has moved an amendment which it proposed that the Cyber Appellate Tribunal constituted under Section 48 of the IT Act would be merged with ***Telecom Disputes Settlement & Appellate Tribunal (TDSAT)*** constituted under Section 14 of the Telecom Regulatory Authority of India (TRAI) Act.

The Cyber Appellate Tribunal has not been functioning since June 2011. The jurisdiction of TDSAT extends to matters that lay before the Cyber Appellate Tribunal and also the Airport Economic Regulatory Authority Appellate Tribunal. The Tribunal exercises original as well as appellate jurisdiction in regard to Telecom, Broadcasting and Airport tariff matters. With respect to cyber matters the Tribunal exercises only the appellate jurisdiction.

1.12 ACTIVITY

Explain the constitution of Cyber Appellate Tribunal along with the latest amendments? What are the powers and functions of TDSAT? (1000 words)

Unit 4: Facets of Cyber Crime: Offences, Penalties and Compensation

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Doctrine of Actus Reus and Mens Rea in Cybercrimes

1.4 Facets of Cyber crime

1.5 Cyber Pornography

1.6 Test determining obscene content

1.7 Present scenario in India

1.8 Cyber Stalking

1.9 Legislative framework and position in India

1.10 Provisions under Indian Penal Code

1.11 Cyber Terrorism

1.12 Famous Incidents of Cyber Terrorism in the world

1.13 Legal provisions under the I.T. Act

1.14 Important provisions under the IT Act, 2000

1.15 Let's sum up

1.16 Further reading

1.17 Check your progress: Possible answers

1.18 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Doctrine of Actus Reus and Mens Rea in Cybercrimes

- Facets of Cyber Crime
- Legislative Framework and Position in India

1.2 INTRODUCTION

The rampant growth and development of Internet and Computer technology have paved the way to new forms of transnational crimes, especially Internet-based. The Indian Legislature does not provide the explicit definition of Cybercrime in any statute. In general, the term cybercrime means any kind of illicit activity which is carried out with the help of the internet or computers. It includes all unauthorized access of information and security breakage like privacy, password etc. with the aid of the Internet. On the whole, Cybercrime is an unlawful act wherein the computer is either used as a tool or a target or both.[43]

1.3 DOCTRINE OF ACTUS REUS AND MENS REA IN CYBERCRIMES

There are two essential elements which constitute a crime i.e., Actus Reus and Mens Rea.

- ***Actus Reus in Cyber Crimes***

  The word 'Actus' connotes a 'mental or spiritual act'. Actus Reus can be defined as "Such result of human conduct as the law seeks to prevent". Actus Reus in case of cybercrimes has become a challenging task as the entire act is committed in intangible surroundings. The element of actusreus is relatively easy to identify, but it is very difficult to prove. One must-see at what state of mind the wrongdoer has committed the crime and must be able to prove that the doer was well aware of the unauthorized access.

- ***Mens Rea in Cyber Crimes***

  Mens Rea is the second essential element in a crime and is known as 'guilty mind'. It refers to the mal-intent of the individual who commits the act. Mensrea in case of Cybercrimes

[43] Jain, Neelesh&Shrivastava, Vibhash& Professor, & Professor, Assistant (2014) "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY" 4

encompasses two elements. Firstly, there must be an 'intent' to secure access to any kind of programme or data held in any computer, computer system or network. Secondly, the person committing such offence must have the knowledge that the access he intends to secure is unauthorized.[44]

1.4 FACES OF CYBERCRIME

- ***Hacking:*** Hacking means unauthorized access/control over a computer system or a computer network. An act of hacking completely destroys the data as well as computer programmes.
- ***E-mail Spoofing:*** A spoofed e-mail is one which misrepresents its origin i.e., it is an e-mail that appears to originate from one source while it actually has been sent from another source. In 2016, Flipkart's CEO BinnyBansal's email account was spoofed.
- ***Trojan Attacks:*** A Trojan is an unauthorized programme which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is via e-mail.
- ***Salami attacks:*** This type of crime is normally prevalent in financial institutions in instances of financial crimes. It is also known as Salami Slicing wherein the attackers use an online database to seize the personal information of the customers such as bank details, credit card details etc. Later, the attackers keep deducting small amounts of money from every account over a stipulated period of time.[45]
- ***Data Diddling:*** Data diddling involves changing of data prior to or during input into a computer i.e., alteration of raw data before a computer processes it and then changing it back after the processing is completed. Section 66 and 43(d) of the I. T. Act, 2000 covers the offence of data diddling. The NDMC Electricity Billing Fraud Case[46] that took place in 1996 is a typical example. A private contractor was made to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized

[44]Etter, B (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide
[45]Etter B (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand
[46]2003 IIAD Delhi 452

accounting, record maintenance and remittance in his bank was misappropriated by manipulating data files to show less receipt and bank remittance.

- ***Intellectual Property Crimes:*** Crimes pertaining to IPR includes software piracy, copyright infringement, trademark violations, theft of computer source code etc. One such crime is Domain Name violations and passing off. In Cardservice International Inc. VsMc Gee[47], it was held that the domain serves the same function as the trademark and is not a mere address or like finding the number on the Internet and, therefore, it is entitled to equal protection as a trademark. It was further held that a domain name is more than a mere Internet address for it also helps identify the Internet site for those who reach it, much like a person's name identifies a particular person.
- ***Phishing and Vishing:*** Phishing means the acquisition of information such as usernames, passwords, credit card details etc. by electronic communication. The information is acquired by using fake emails or fake messages which contain link of virus / malware infected fake websites. This kind of websites request the users to enter all their personal details. On the other hand, Vishing is typically used to steal credit card numbers or other kind of information from the users for use in instances of identity theft.[48]

1.5 CYBER PORNOGRAPHY

The word 'Pornography' has no specific definition in the eyes of law as every country has its own customs and traditions. Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials The act pornography is made legal in some countries but in others, it is illegal and banned. The Indian legal system has been structured in such a way that it contains provisions to criminalize any kind of scatological content.[49] Legalization of Child Pornography doesn't come under the purview of

[47] *Cardservice International Inc vMc Gee*, 42 USPQ 2d 1850

[48] Eric JSinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2

[49] See e g The Post Office Act, 1893 (prohibits obscene matters being transmitted through post); The Sea Customs Act, 1878 (prohibits the import of obscene literature); The Dramatic Performances Act, 1876 (prohibits obscene plays); The Cinematograph Act, 1952 (makes provisions for censorship of films); The Press Act, 1951 (prohibits grossly indecent, scurrilous or obscene publications); The Indecent Representation of Women (Prohibition) Act, 1986 (prohibits obscene photographs of women)

pornography as a whole. Child Pornography at the very instance is a felonious act and is one of the heinous crimes that has eventually led to other severe crimes such as sex tourism, sexual abuse of child etc. The obscene contents involving children creates a major threat to the development and security of children which initiates a path for sexual abuse of children. The concepts of obscenity and pornography oscillate from time to time and from country to country. Although the terms obscenity and pornography are different, they are related to each other.

1.6 TEST DETERMING OBSCENE CONTENT

The test of obscenity was first laid down in ***Regina VsHicklin***[50] ***(also known as Hicklin's test***i.e., a content is obscene if "the tendency of the matter charged with obscenity is to deprave and corrupt those whose minds are open to such immoral influences and whose hands a publication may fall". This approach was later adopted even in India in the case of ***Ranjit Singh UdeshiVs State of Maharashtra***[51] with regards to a sale of an allegedly obscene magazine.

After the Hicklin's Test, the U.S Supreme Court went against the said rule and established a new set of principles called as the ***Community Standards Test*** **in** ***Roth Vs. United States***[52] and held that "obscene material was not protected by the First Amendment and could be regulated by the States rather than by a singular, Federal standard and also a new judicial standard for defining obscenity that invoked the average person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeals to prurient interest". Furthermore, the Supreme Court held that in order to decide how obscenity derived, we need to consider the following five-part structure:-

- The perspective of evaluation is that of an ordinary, reasonable person.
- Community Standards of acceptability are used to measure obscenity.
- Obscenity law only applies to the works whose themes are in question.
- A work, in order to be evaluated for obscenity, has to be taken in its entirety.

[50] *Regina vHicklin* [1868] LR 3 QB 360
[51] *Ranjit Singh Udeshi v State of Maharashtra* AIR [1965] SC881
[52] *Community Standards Test* in *Roth v United States*[1957]354 U S476

- An obscene work is one that aims to excite individuals' prurient interest.

However, in ***Samresh Bose VsAmalMitra***[53]**,**the Supreme Court held that 'vulgar writing is not necessarily obscene'. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novels; whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences. In the instant case, the court had differentiated between vulgarity and obscenity and further held that while judging the question of obscenity 'the Judge should place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers'.

This Community Standards Test was also used in India in, ***K.A. Abbas Vs Union of India***[54]which stated that;

- The dominant theme taken as a whole, appeals to prurient interests according to the contemporary standards of the average man;
- The motion picture is not saved by any redeeming social value; and
- It is patently offensive because it is opposed to contemporary standards.

Later, the Millers Test was brought to light which was a developed form of Community Standards Test. The Millers Test took birth from the case of ***Miller Vs California***[55]whereinThe Supreme Court of United States provided the basic guidelines and three-point tests to determine obscenity in the work. They are as follows:-

- That the average person, applying contemporary 'community standards', would find that the work, taken as a whole, appeals to the prurient interest.
- That the work depicts or describes, in an offensive way, sexual conduct or excretory functions, as specifically defined by applicable state law or applicable law.
- That the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

[53] *Samresh Bose vAmalMitra* AIR [1986] SC 967
[54] *K.A. Abbas v Union of India* AIR [1971] SC481
[55] *Miller v California* 413 US 15 [1973]

1.7 PRESENT SCENARIO IN INDIA

The Supreme Court of India presently adopts the *Community Standards Test* as a measure of detecting obscene content. In ***AveekSarkar V. State of West Bengal***[56]**,** the facts of the case revealed that a German magazine published an article about a tennis player picturing him naked with his fiancé as a stand against racism and to show that love champions over everything. The Supreme Court found the respondents innocent of the charges levied against them and held that in a situation like this Hicklin's test cannot be used and the only measure to be implemented is the community standards test; and it further stated that the photograph must be viewed in the context of the message which the photograph appears to convey, and not in isolation. The Supreme Court further instructed that a more adaptive community standards test must be applied for a continuously evolving society like India.

Under the ***Information Technology Act, 2000, Section 67***of the Act states that publishing obscene content online is punishable with imprisonment of three years and a fine of rupees five lakhs; and subsequent conviction will lead to a punishment of imprisonment of five years and fine of ten lakh rupees. However, under the ***Information technology (Amendment) Act, 2008, section 67(A)*** it has been made clear that a publication of sexual content will lead to a punishment of five years' imprisonment on the first conviction with a fine of rupees ten lakh and a punishment of 7 years with a fine of rupees ten lakh on the subsequent conviction. ***Section 67(B)*** of the amendment which is against child pornography makes it clear that not only publication and viewing but also possession of such pornographic content is punishable with five years' imprisonment and ten lakh rupees on the first conviction and seven years' imprisonment and ten lakh rupees on the subsequent conviction.

1.8 CYBER STALKING

Cyber Stalking has been defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone. It is an advanced form of stalking which is committed over

[56] *AveekSarkar v State of West Bengal*[2014] 4 SCC257

the online medium.[57] It involves a conduct of harassing or threatening an individual in order to gather information about the victim. Cyber Stalking can be conducted via email, internet and computer. The Internet provides an opportunity for the stalkers to keep a check on the activities of their victims and the risk factor is comparatively less compared to physical stalking as the identity of the stalker can be hidden.

1.9 LEGISLATIVE FRAMEWORK AND POSITION IN INDIA

Cyber Stalking gathered importance after the evolution of the internet. California was the first state to pass the anti-stalking law in 1990. The gravity of cyber stalking came into focus in India with the ***Manish Kathuria Case.***This was first reported case cyber stalking case in India and it was the reason the provisions pertaining to cyber stalking were included in the Information Technology (Amendment) Act, 2008. The Delhi Police arrested Manish Kathuria for stalking a person called RituKohli by illegally chatting with her name on 'www.mirc.com' website. As a result, the victim started receiving obscene calls from various parts of India and abroad. The matter was reported to the Delhi Police wherein a case registered under Section 509 of the Indian Penal Code for outraging the modesty of a women.[58] However, the said section does not cover cyber stalking. This case was an alarm to the Government and as a result ***Section 66A of the Information Technology (Amendment) Act, 2008 i.e., Punishment for sending offensive messages through communication service, etc.***The offences like obscenity, defamation, bullying etc. came under the purview of the said section.

However, the aforesaid section was struck down in the year 2015 in the writ petition ***ShreyaSinghalVs Union of India[59].*** The Apex Court struck down Section 66A of Amendment Act, 2008 as it was misused by the authorities to the effect of violating ***Article 19(1) of the Constitution of Indiai.e., Freedom of Speech and Expression.***

[57]Kabay, M E (2000) Studies and Surveys of Computer Crime, Focus <http://securityportal.com/cover/coverstory2001211.html>

[58] Section 509 of IPC states that, Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both

[59]*ShreyaSinghal v Union of India*WP (Crl) No 167 of 2012

At present, ***Section 72 and Section 72A*** of the Information Technology (Amendment) Act, 2008 regulate cyber stalking. Section 72 of the Act pertains to Penalty for breach of confidentiality and privacy and Section 72A of the Act deals with punishment for disclosure of information in breach of lawful contract.

1.10 PROVISIONS UNDER INDIAN PENAL CODE

There are no direct provisions that deal with the issue of cyber stalking. However, there are certain provisions under the Indian Penal Code that have some linkage with cyber stalking.

a) Section 354D defines 'Stalking'. It states that, any man who,

- follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

b) Section 292 defines 'Obscenity'. It states that, the act of sending obscene materials to the victim on a social networking site or through emails or messages etc. or deprave the other person by sending any obscene material using the internet with the intention that the other person would read, see or hear the content of such material, shall amount to the offense under the said section being committed.

c) Section 507 relates to 'Criminal Intimidation by anonymous communication'. It states that, when the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat comes, it amounts to an offence. This satisfies the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty if he attempts to conceal his/her identity.

d) Section 354C defines 'Voyeurism'. It states that, any man who watches, or captures or disseminating the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator.[60]

[60] KPMG (2000) , E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation, USA

1.11 CYBER TERRORISM

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. It is a combination of cyberspace and terrorism. There isn't an appropriate definition for Cyber Terrorism which can be accepted worldwide. However, a universally acknowledged definition of Cyber Terrorism is 'A criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and / or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda'.[61]

1.12 FAMOUS INCIDENTS OF CYBER TERRORISM IN THE WORLD

- ***Attack on the Indian Parliament***

The Indian Parliament was attacked by a cyber-attack on 13th December, 2001. The attackers used new technology and committed forgery to fulfil their end. They forged the gate pass and for the attack they downloaded the official logo of Ministry of Home Affairs, other documents and the layout of the Parliament building. Police found a laptop from main accused Mohammed Afzal and ShaukatHussain Guru. The Police officials established that they have accessed the internet through Pakistan based Internet Service Providers (ISP). Additionally, the Investigating officers found incoming and outgoing cell phone call numbers of deceased terrorists and a satellite connection with deceased terrorist's cell phone.[62]

- ***Yugoslavia Conflict***

[61] Russell G Smith, Peter Grabosky and GrgorUrbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press

[62] SayantanChakravarty, "Parliament attack well-planned operation of Pakistan-backed terror outfits, evidence shows", India Today, December 31st 2001

When NATO[63] air strikes hit the Former Republic of Yugoslavia in Kosovo and Serbia, NATO web servers were subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to 'ping saturation', Distributed Denial of Service (DDoS)[64] assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of the American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks caused serious disruption of NATO communications infrastructures.

- ***Epsilon***

Epsilon was one of the costliest cyber-attacks in history. Epsilon was the world's largest provider of marketing and handling services to industry giants such as JP Morgan Chase, Best Buy, and other major financial service providers, retailers and other major companies in 2011. It had an estimated damage cost that ranged from $225 million to $4 billion dollars. Names and email addresses were stolen from Epsilon, the world's largest email marketing firm in 2011, which handled more than 40 billion emails every year, more than 2,000 brands worldwide including Marks and Spencer. The company faced a spear phishing attack, a sophisticated fraud which aims to gather user details by sending emails from a trusted company with many users, such as PayPal. So, in the attack, the hackers targeted the email addresses that they could use for their criminal activities, making the implications a lot greater than estimated.

- ***Sony PlayStation Network, Microsoft's Xbox Live Network Case***

In this case, the confidential data of the employees and their families were leaked in 2014. The company faced a huge loss in revenue due to the publication of employee information which included their salaries, social security numbers, and executive emails. Due to this, an attack was launched by the *'Lizard Squad'*, a cyber-terrorist against the Tor Project, a

[63]The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party

[64] One common form of DOS and DDOS attacks use a technique known as ping saturation. Ping is a simple Internet utility used to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests

network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure wherein the network had gone down for almost 10 hours.

1.13 LEGAL PROVISIONS UNDER THE I.T. ACT

A new ***Section 66F*** was inserted by the Information Technology (Amendment) Act, 2008. Prior to the aforementioned provision, there was no specific provision in the IT Act, 2000 that dealt specifically with Cyber Terrorism.

Section 66F relates to 'Punishment for cyber terrorism'.[65]It stated that,

Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

- denying or cause the denial of access to any person authorized to access computer resource; or
- attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
- introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

- knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer

[65] Section 66F, Information Technology (Amendment) Act, 2008

database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

1.14 IMPORTANT PROVISIONS UNDER THE I.T. ACT, 2000

SECTIONS	OFFENCES	PENALTIES
Section 65	**Tampering with computer source documents**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66	**Hacking the computer system with intent or knowledge**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66B	**Misappropriation of information stolen from computer or any other electronic gadget**	**Imprisonment up to 3 years or fine up to 1 lakh rupees or both.**
Section 66C	**Stealing someone's identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**
Section 66D	**Accessing personal data of someone with the help of computer by concealing their identity**	**Imprisonment up to 3 years or fine up to 1 lakh rupees**

Section 66E	**Breach of Privacy**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 66F	**Cyber Terrorism**	**Imprisonment which may extend to imprisonment of life.**
Section 67	**Publication of obscene information in e-form**	**Imprisonment up to 5 years and fine up to 1 lakh rupees.**
Section 67A	**Publishing or circulating sex or pornographic information through electronic means**	**Imprisonment up to 7 years or fine up to 10 lakh rupees.**
Section 67B	**Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode**	**Imprisonment up to 5 years or fine up to 10 lakh rupees.**
Section 68	**Failing to comply with the directions of the controller**	**Imprisonment up to 3 years or fine up to 2 lakh rupees or both.**
Section 71	**Misrepresentation**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72	**Breach of confidentiality and privacy**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 72A	**Disclosure of information**	**Imprisonment up to 3 years or fine up to 5**

	in breach of lawful contract	**lakh rupees or both.**
Section 73	**Publishing false digital signature certificate and false in certain particulars**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**
Section 74	**Publication for fraudulent purposes**	**Imprisonment up to 2 years or fine up to 1 lakh rupees or both.**

1.15 LET'S SUM UP

In this chapter, we have studied about the varied facets of cybercrimes along with the legislative framework and position in India. We have also seen the provisions under IPC with respect to Cybercrime offences. Finally, we have ended the discussion with the famous incidents of cyber terrorism in the world and the important provisions under I.T. Act, 2000.

1.16 FURTHER READING

- S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81
- Rhiannon Williams, "The Biggest Ever Cyber Attacks and Security Breaches", The Telegraph, Available on http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggestever-cyber-attacks-and-security breaches.html.
- See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are cybercrimes?

Cybercrimes are illegal acts in which a computer is made a tool or object whereby the means or purpose of committing it involves influencing the function of a compute; or instances involving computer technology wherein unethical or unauthorized behaviour relating to the automatic transmission of data results in creating victims and perpetrators.

2. What are the various facets of cybercrime?

The various facets of cybercrime are as follows:

- Hacking
- Email spoofing
- Trojan attacks
- Salami attacks
- Data diddling
- Intellectual property related crimes
- Phishing and vishing

3. What is cyber pornography?

Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

4. What is cyber stalking?

Cyber Stalking is an advanced form of stalking committed over online medium and can be defined as a crime wherein the stalkers use the internet or any other electronic device to stalk someone.

5. What is cyber terrorism?

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives.

1.18 ACTIVITY

Infer the reason that Information Technology Act is a *'Cyber Crime Friendly Act'*.(1500-2000 words.

Block 2

Digital Signature, Electronic Signature and Laws Related to Certifying Authority of India

Unit 1: Digital and Electronic Signature: Concept and Procedure

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Concept of Public and Private key

1.4 Important terms related to digital signature

1.5 Creation and Verification of a digital signature

1.6 Digital Signature and Public Key Infrastructure

1.7 Process of Public key Infrastructure

1.8 Difference between an electronic and digital signature

1.9 Legal Provisions related to digital and electronic signature

1.10 Adoption of Security Procedures and The IT Act, 2000

1.11 Let's sum up

1.12 Further reading

1.13 Check your progress: Possible answers

1.14 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter,you should be able to understand:

- Concept of Public and Private key
- Digital and Electronic signature
- Legal provisions with regard to digital and electronic signature

1.2 INTRODUCTION

Digital signature and electronic signature are used interchangeably but they are not the same. Digital signature is a mere subset of e-signature. Digital signatures are based on asymmetry, or public key, cryptography and are capable of fulfilling the demand of burgeoning e-commerce by not only providing message authentication, integrity and non-repudiation function but also making it highly scalable. Digital Signatures are basically ***'enciphered data'*** created using cryptographic algorithms. It is not a digitalized image of a handwritten signature. Digital signatures are an actual transformation of an electronic message using public key cryptography. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm).[66]

On the other hand, an electronic signature includes all types of electronically approved methods. It could be a graphical stamp, a process or even pressing the 'Agree' button in the terms and conditions etc. It includes simple forms like pressing ***'place order'*** to complex forms like a biometric signature.

1.3 CONCEPT OF PUBLIC AND PRIVATE KEY

Before digitally signing an electronic communication, the sender has to create a public-private key pair. There are two keys used for digital signatures i.e., Private key and Public key.[67] The private key is kept confidential by the signer and used by him only to create the digital signature whereas the public key is more widely known and is used to verify the digital signature by the relying party.

1.4 IMPORTANT TERMS RELATED TO DIGITAL SIGNATURE

"Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature. (Section 2(1) (d) of IT Act, 2000)[68]

[66]The control implications of a public key infrastructure <https://repository.up.ac.za/dspace/bitstream/handle/2263/4067/Bouwer_Control(1999).pdf?sequence=1&isAllowed=y>

[67] Adams, C, [1999] "Understanding Public-key Infrastructure", Macmillan Technical Publishing

[68]Certifying Authorities - Digital Signature Certificates <http://www.digitalsignaturesale.com/certifying-authorities/>

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. (Section 2(1) (f) of IT Act, 2000)

"Certifying Authority" means a person who has been granted a license to issue an electronic signature certificate under Section 24. (Section 2(1) (g) of the IT Act, 2000)

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3. (Section 2(1) (p) of the IT Act, 2000)

"Electronic Signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature. (Section 2(1) (ta) of the IT Act, 2000)[69]

"Electronic Signature Certificate" means an Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate. (Section 2(1) (tb) of the IT Act, 2000)

"Key Pair" is an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key. (Section 2(1) (x) of the IT Act, 2000)

"Private Key" means the key of a key pair used to create a digital signature. (Section 2(1) (zc) of the IT Act, 2000)

"Public Key" means the keyof a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Section 2(1) (zd) of the IT Act, 2000)

1.5 CREATION AND VERIFICATION OF A DIGITAL SIGNATURE

A digital signature is a two-way process, involving two parties, the signer (creator of the digital signature) and the recipient (verifier of the signature). A digital signature is complete, if and only if, the recipient successfully verifies it.[70]

[69] ICAI members use electronic signature for signing audit <https://taxguru.in/chartered-accountant/icai-members-may-use-electronic-signature-signing-audit-reports.html>

- ***Creation of a digital signature***

- The signer demarcates what is to be signed. The delimited information to be signed is termed as the 'message'.
- A hash function[71] in the signer's software computes a hash result (digital fingerprint) unique to the message.
- The signer's software then transforms (encrypts) the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.
- The digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. Since a digital signature is unique to its message, it is useful if it maintains a reliable association with its message.

- ***Verification of a digital signature***

Recipient:

- Receives digital signature and the message
- Applies signer's public key on the digital signature
- Recovers the hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Computes a new hash result of the original message by means of the same hash function used by the signer to create the digital signature
- Compares the hash results recovered[72]

If the hash result computed by the verifier is identical to that of the hash result extracted from the digital signature during the verification process, it indicates that the message remained unaltered and vice versa.

Verification is a two-prong process i.e.,

---

[70]American Bar Association Digital Signature Guidelines <https://horseproject.wiki/index.php/American_Bar_Association_Digital_Signature_Guidelines>

[71] A 'hash result' is used in both creating and verifying a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value or hash result of a standard length which is usually much smaller than the message

[72]Top Compelling Reasons Fedena Blog <https://fedena.com/blog/2019/06/top-compelling-reasons-why-your-school-website-must-have-an-ssl-certificate.html>

- to verify whether the signer's private key was used to digitally sign the message and
- to verify whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.6 DIGITAL SIGNATURE AND PUBLIC KEY INFRASTRUCTURE

The digital signature regime operates online without any human intervention. The Sender sends a digitally signed message and the recipient receives and verifies it. The requirement is that both the sender and the receiver must have the digital signature software at their respective ends. This paves way for the participation of a ***Trusted Third-party (TTP)***to certify the subscriber's identity and their relationship to their public keys. The Trusted Third Party is referred to as a Certifying Authority (CA). The main function of the certifying authority is to verify and authenticate the identity of the subscriber i.e., a person in whose name the digital signature certificate is issued.[73]

A Digital Signature Certificate securely binds the identity of the subscriber. It contains the name of the subscriber, his public key information, name of the certifying authority who issued the certificate, its public key information and the validity of the certificate. These certificates are stored in an online publicly accessible repository maintained by the Controller of certifying authorities or in the repository maintained by the certifying authority. Every Certifying Authority must maintain a repository[74] for the certificates as per the Certification Practice Statement (CPS).

Under the Information Technology Act, 2000, *Section 35 to 40* lay down the procedure for issuance, rejection, suspension and revocation of digital signature certificates. They provide that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government and different fees may be prescribed for different classes of applicants. Furthermore, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

[73]Tarek A El-Mageed, Nariman A El-Salam, [2004] "Public Key Cryptosystems and its Applications in Digital Signature" The 2nd International Conference on Informatics and System INFOS2004, Cairo-Egypt

[74] A repository maintains an up-to-date list of all the valid digital signature certificates, and also a list of suspended or revoked certificates

Digital signatures fulfil all statutory requirements associated with the acceptance of handwritten signatures. The law does not recognize the digital signature in a stand-alone environment. It gives recognition to the whole system – the public key infrastructure including the standards, which create and verify digital signatures. Digital signature establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the signer of an electronic message and also confirms that the said signer approved the content of an electronic message.[75]

1.7 PROCESS OF PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world. The process is as follows:-

- Subscriber applies to Certifying Authority for Digital Signature Certificate.
- The Certifying Authority verifies the identity of the subscriber and issues the digital signature certificate.
- The Certifying Authority forwards the digital signature certificate to the repository maintained by the controller.
- Subscriber digitally signs an electronic message with the private key to ensure sender authenticity, message integrity, and non-repudiation and sends it to the relying party.
- The relying party receives the message, verifies the digital signature with the subscriber's public key and goes to the repository to check the status and validity of the subscriber's certificate.
- Repository does the status check on the subscriber's certificate and reverts back to the relying party.

Under the IT Act, Sections 17 to 34 provide a system for regulation of certifying authorities, to exercise supervision over the activities of certifying authorities and also lay down principles and conditions regulating the certifying authorities.

[75]CH Magazine | VARIOUS AUTHORITIES UNDER THE IT ACT <https://www.chmag.in/articles/legalgyan/various-authorities-under-the-it-act/>

1.8 DIFFERENCE BETWEEN ELECTRONIC AND DIGITAL SIGNATURE

CRITERIA	ELECTRONIC SIGNATURE	DIGITAL SIGNATURE
Definition	**It is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record.[76]**	**It is a term for one technology-specific type of electronic signature.**
Technology	**They can take many forms and can be created by many different technologies. It permits a broad range of 'electronic signatures' to satisfy the requirements of a legal signature.**	**It involves the use of public-key cryptography (asymmetriccryptography) to 'sign' a message.**
Example	**A name typed at the end of an email message by the sender, PIN used in ATM cards to identify the sender to the recipient etc.**	**It is a block of data at the end of an electronic message that attests to the authenticity of the said message. Digital Signatures are a transformation of an electronic message using public-key cryptography.**

[76] Legal Recognition to Electronic records in India <https://scholarticles.wordpress.com/2015/08/27/legal-recognition-to-electronic-records-in-india/>

1.9 LEGAL PROVISIONS RELATED TO DIGITAL AND ELECTRONIC SIGNATURE

The Information Technology Act, 2000 provides a legal framework to authenticate electronic records. The Act facilitates and safeguards electronic transactions in the electronic medium. It is based on UNCITRAL's Model Law on E-commerce, which adopts 'functional equivalent approach' advocating a shift from a paper-based environment to computer-based.[77]

- ***Section 3*** gives legal recognition to electronic records and digital signatures. ***Section 3A*** was inserted by the IT (Amendment) Act, 2008 which in turn allowed electronic signatures to be used for authentication of e-records. Section 3 provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The authentication of the electronic record shall be effected by the use of the asymmetric cryptosystem and hash function which envelops and transform the initial electronic record into another electronic record.
- ***Section 5*** provides for legal recognition of electronic signature. It states, where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.
- ***Section 6*** deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- ***Section 14*** deals with secure electronic records. It states that, where any security procedure has been applied to an electronic record at a specific point of time, such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
- ***Section 15*** provides for situations when an Electronic Signature can be considered as secure.

[77] Digital Signature | Ministry of Electronics <https://meity.gov.in/content/digital-signature>

- ***Section 16*** provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability, and cost of alternative procedures, the volume of similar transactions entered into by other parties etc.

1.10 ADOPTION OF SECURITY PROCEDURES AND THE IT ACT, 2000

The main purpose of the IT Act, 2000 is to secure electronic records ***(Section 14)*** and secure electronic records ***(Section 15)*** by applying appropriate security procedures.

Section 14 advocates application of any security procedure to make the electronic record secure. A secured electronic record shall be deemed to be a secured electronic record from the time the said security procedure is applied to the time of its verification. It is important to note that the onus of securing an electronic record rests with the creator of the said record. The presumption is that an electronic record is a secured one from the specific point of time when any security procedure has been applied to it to the time of its verification at the recipient's end, till the recipient proves it otherwise.

Section 15 lays down the security features for a subscriber-specific electronic signature, which includes digital signature as well. It provides for 2 specific features:-

- Signature creation data under the exclusive control of signatory or linked to the signatory (the authenticator) and to no other person and
- Storage and affixation of signature creation data as per prescribed processes.[78]

Section 16 of the act enunciates about security procedure. It is proactive in nature as it gives liberty to the Central Government to adopt and assimilate any technology for providing a regime of secure electronic record and electronic signature. This section puts an onus on the Central

[78]Afrianto, Irawan&Heryandi, Andri&Finandhita, Alif&Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

Government to prescribe the security procedure is having regard to commercial circumstances, nature of transaction and other related factors as it may consider appropriate before adopting such security procedures and practices.[79] The lawmakers have made the Act flexible in terms of technology adoption and assimilation, which would further influence both e-commerce and e-governance transactions. Thedigital payments ecosystem in India has already been revolutionized without even taking cognizance of *Sections 14-16 of the Act.* There are Rules and Regulations pertaining to and for the purpose of regulating the functioning of Certifying Authorities. It lays down procedure and standards (rule 3-8) for securing electronic records and digital signatures. Under ***Rule 3 of the Information Technology (Security Procedure) Rules, 2004***an electronic record shall be deemed to be a secure electronic record for the purpose of the act if it has been authenticated by means of a secure electronic signature.[80]

1.11 LET'S SUM UP

In this chapter, we have studied the concept of public and private key along with the important terms with respect to digital signature. We also saw how a digital signature is created and verified and the difference between digital and electronic signature. Finally, we have ended our discussion with legal provisions pertaining to digital and electronic signature and adoption of security procedures with respect to it.

1.12 FURTHER READING

- https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf
- http://www.ijhssnet.com/journals/Vol_6_No_12_December_2016/7.pdf
- http://www.ijarcs.info/index.php/Ijarcs/article/viewFile/2484/2472

[79] Stamp, M [2011] "Information Security: Principles and Practice" Second Edition, John Wiley and Sons
[80] Banerjee, Arindam (2016) The Impact of Electronic Signatures on Internal Control Systems

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a digital signature?

Digital signatures are based on asymmetry, or public key, cryptography and are basically *'enciphered data'* created using cryptographic algorithms, and are actual transformations of electronic messages using public-key cryptography.

2. What are the differences between an electronic signature and digital signature?

Electronic signature is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record while a digital signature is a term for one technology-specific type of electronic signature while, digital signatures involve the use of public-key cryptography (asymmetric cryptography) to 'sign' a message.

3. Mention some legal provisions related to the digital and electronic signature?

Some of the legal provisions related to the digital and electronic signature are as follows:

- Section 3 of the Information Technology Act, 2000 which gives legal recognition to electronic records and digital signatures
- Section 5 of the Information Technology Act, 2000 which provides for legal recognition of electronic signature.
- Section 6 of the Information Technology Act, 2000 which deals with the use of Electronic Records and Electronic Signature in the context of Government and its agencies.
- Section 16 of the Information Technology Act, 2000 which provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures.

4. What is public key infrastructure?

Public Key Infrastructure is about the management and regulation of key pairs by allocating duties between contracting parties (certifying authorities/subscribers) laying down the licensing and business norms for certifying authorities and establishing business processes to construct contractual relationships in a digitalized world.

5. How is a digital signature verified?

The verification of a digital signature involves the following steps:

i. Verifying whether the signer's private key was used to digitally sign the message; and
ii. Verifying whether the newly computed hash result matches the original hash result which was recovered from the digital signature during the verification process.

1.14 ACTIVITY

Describe the legal provisions pertaining to digital and electronic signature along with the security procedures in I.T. Act, 2000. (800 words)

Unit 2: Digital Signature Certificate

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Types and Classes of Digital Signature Certificate

1.4 Certifying Authority

1.5 Utility of Digital Signature Certificates

1.6 Ingredients of a Digital Signature Certificate

1.7 Subscriber's Obligations

1.8 Disadvantages of Digital Signature Certificates

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Digital Signature Certificate
- Types and Classes of Digital Signature Certificates
- Certifying Authorities issuing digital signatures
- Advantages and disadvantages of Digital Signature Certificates
- Statutory provisions related to Digital Signature Certificates

1.2 INTRODUCTION

A Digital Signature Certificate is a digital key used to validate and certify the identity of an individual digitally. Such a digital Signature Certificate is issued by a certifying authority. Digital Signature Certificates are created by use of public-key encryptions and form the digital equivalent of physical certificates in electronic format. Digital Signature Certificates form a useful way of signing documents electronically. Similar to physical documents being signed manually, Digital Signature Certificates serve the purpose of digitally signing electronic documents. As per the provisions of the Information Technology Act, 2000, Digital Signature Certificates are considered to be admissible in a court of law.[81] Such Digital Signature Certificates can stay valid for upto a minimum of one year to a maximum of three years. Digital Signature Certificates can be used by both individuals and/or organizations. Digital Signature Certificates function based on MD5 algorithm associated with cryptography, which is, in essence, a 'Message-Digest Algorithm', that receives a message of any length as input and releases as output a 128-bit result which is a 'message digest' based on the input.[82]

Today, India is one of the few nations that have laws associated with Digital Signature Certificates. As per the existing laws, all authorized signatories of organizations and any other professional having the authority to *inter alia* sign documents shall be required to obtain the Digital Signature Certificates. Such group of persons could include but not be limited to directors of companies, auditors or chartered accountants, practising company secretaries or those engaged in jobs, officials working at banks etc. Once the Digital Signature Certificate has been issued and received by the applicant, the certificate can be used by the holder to sign any document online.

1.3 TYPES AND CLASSES OF DIGITAL SIGNATURE CERTIFICATES

There can be four kinds of Digital Signature Certificates, which are as follows:

(a) ***Sign*** – Sign Digital Signature Certificates can be solely used for signing documents. While on one hand, its usage signifies integrity of the data as well as the signer, on the

[81]FeghhiJ and P Williams, Digital Certificates: Applied Internet Security 1st ed Reading, MA: Addison-Wesley [1999]
[82]StallingsW, Cryptography and Network Security, 3rd ed. EnglewoodCliffs, NJ: Prentice-Hall, 2002

other, it ensures that the data does not get altered or tampered. Commonly, Digital Signature Certificates are used with respect to the filing of tax returns.[83]

(b) ***Encrypt*** – Encrypt Digital Signature Certificates can solely be used to encrypt a document, as popularly used by companies to encrypt and upload documents and/or send across classified information. Encrypt Digital Signature Certificates are used in association with e-commerce documents and other documents, legal or otherwise, that are extremely confidential in nature and need extensive protection.

(c) ***Sign and Encrypt*** – Sign and Encrypt Digital Signature Certificates can be used to together serve the individual purposes of each of sign and encrypt Digital Signature Certificates. It helps authenticate information as well as maintain their confidentiality at the same time.

(d) ***Server Certificate*** – These kinds of certificates are used in identifying a server by means of the hoist name and/or IP address that they contain, and are used for ensuring secure communication of data using the internet.

Primarily, there could be three classes of Digital Signature Certificates. They are as follows:

(a) Class 1 Certificate – These Digital Signature Certificates are issued to individuals and/or private users to authenticate the details of the user such as name, email address etc.

(b) Class 2 Certificate – These Digital Signature Certificates can be issued to individuals as well as organizations for both personal as well as professional use. The purpose of its use is to reaffirm and authenticate the details of the signer. It is used most commonly n instances of electronic form filling, income tax filing, registration is done online, email attestation, application for GST etc.

(c) Class 3 Certificate – These Digital Signature Certificates are high assurance certificates that more secure in comparison to Class 2 Certificates, and are arguably considered to be the safest. They provide high safety and security with respect to information and are used mainly in e-commerce and online trading involving privileged information and big amounts of money. Class 3 Digital Signature Certificates are only issued once the holder makes a physical appearance before the certifying authority.[84]

[83]Denning, D E Cryptography and Data Security. Reading, MA: Addison-Wesley(1982)

[84] Stallings, W Cryptography and Network Security: Principles and Practice, 4th ed Englewood Cliffs, NJ: Prentice Hall(2006)

*

Class 1	Class 2	Class 3
Certificates are issued to government organizations, business organizations as well as individuals.	**Certificates may be issued to those individuals who belong to business and/or government organizations that are willing to verify the information submitted by such individual subscriber. Certificates can also be issued to organizations that are well-known and are capable of self-verifying the information submitted.[85]**	**Certificates can be issued to both individuals as well as organizations.**
Used to enhance the security associated with personal emails and personal web browsing, and is used primarily to that effect.	**Used for aiding in an organization's administrative and functional needs.**	**Used extensively for e-commerce applications, electronic banking, other online services that rely on online memberships and subscription, etc.**
Assurance provided is of the lowest level in comparison to other kinds of certificates.	**Assurance provided is of more than Class 1 certificates. However, the verification process**	**The validation procedure involved provides assurances stronger than that provided by Class 1**

[85] Practical Security Aspects of Digital Signature Systems: Florian Nentwich, EnginKirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna(JUNE2006)

	involved with the issuance is more rigorous than that involved in association with Class 3 certificates.	**and Class 2 certificates.**
Certificates help in confirming a user's name and email address.	**A digital certificate signed by the Certifying authority is given to the head of an organization or his/her nominee so that the process of issuing further Certificates can be initiated.**	**Significant assurances associated with the identity of subscribers are provided following the personal physical appearance of such subscribers before the certifying authority.**

While the certifying authority has the right to issue more classes of certificates, it has to be nevertheless ensured that the same be expressly defined along with their purpose as and when issued.[86]

In order for a Class 3 Certificate to be issued, certain requirements that need being fulfilled are as follows:

Individual Applicant	**Company Applicant**	**Government Applicant**
After the application is filled and submitted, the individual applicant will need to be present physically before the Registration Authority with an original copy of one of the following	**An individual representing the company that has subscribed for the certificate has to be present physically before the Registration Authority with proof of ownership and other details**	**An individual representing a government applicant that has subscribed for the certificate has to be present physically before the Registration Authority with a letter on the official letter of the subscriber**

[86]Banday, M Tariq &Dethe, C (2011) Easing PAIN with Digital Signatures. International Journal of Computer Applications

documents : **i) Passport** **ii) Voter ID Card** **iii) PAN Card** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**associated with the subscriber company.** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**	**which must contain the following:** i) **Name of the organization** ii) **Administrative department** iii) **Address of the subscriber** **In the event a server certificate is applied for, the proof of registration of the domain name shall also have to be submitted.**

1.4 CERTIFYING AUTHORITY

A ***'Certifying Authority'*** is an entity who has been granted the authority of issuing Digital Signature Certificates as per the provisions of section 24 of the Information Technology Act, 2000. All the licensed Certifying Authorities and their contact numbers are available in the public domain.

A Certifying Authority can directly be approached by an applicant with supporting documents of original and self-attested copies for acquiring a Digital Signature Certificate. A Certifying Authority could also be approached for a Digital Signature Certificate also with only the eKYC based authentication details associated with Aadhar Card in which case no supporting documents shall be required. A letter containing the necessary information issued and certified by the bank wherein the applicant of the Digital Signature Certificate holds an account is also considered valid and sufficient for acquiring a Digital Signature Certificate.[87]

[87]Afrianto, Irawan&Heryandi, Andri&Finandhita, Alif&Atin, Sufa. (2019). E-Document Autentification With Digital Signature For Smart City : Reference Model

The applicant of a Digital Signature Certificate holds a private key that corresponds to the public key that is to be listed in the certificate, and further holds a private key which creates the digital signature. The public key which is listed in the Digital Signature Certificate is used to verify the digital signature that the applicant affixes using the secure private key. Once applied, the Certifying Authority could take around three to seven working days for issuing a Digital Signature Certificate.

1.5 UTILITY OF DIGITAL SIGNATURE CERTIFICATES

The utility of Digital Signature Certificateslies in the fact that Digital Signature Certificates can be used as a means of electronic proof of identity of an individual. Digital Signature Certificates can be further used for signing documents digitally or accessing information or availing services over the internet.[88]

Digital Signature Certificates further provide benefits of privacy to their holders and also help authenticate and authorize entities to get involved *inter alia* in electronic transactions.While on one hand Digital Signature Certificates and their usage have been given legal validity owing to the provisions of the Information Technology Act, 2000, on the other, they can also provide a high level of security for online transactions by encrypting information only for the purposes of intended use by the intended recipient(s). The added advantage with respect to Digital Signature Certificates ensures that the information involved remain unaltered in spite of transition.[89]

The major advantages associated with the use and implementation of a Digital Signature Certificate are as follows:

(i) Prevention of Fraud – Use of Digital Signature Certificate eliminates the possibility of fraud by entirely eliminating the scope of alteration therein or creating a duplicate thereof.

(ii) Preserving integrity – Use of Digital Signature Certificates established the validity of a document in all legal, formal and official aspects.

[88]Zheng Y, Imai H and Imai, H (Ed) 2007 Public Key Cryptography, Springer, ISBN: 9783540656449

[89] FIPS (1996) Digital Signature Standard (DSS), FIPS PUB 186-3, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-890, available online at: <http://csrc.nist.gov/publications/fips/fips186-3/fips_186- 3.pdf>

(iii)Advantages in Online Banking – Businesses depending on online banking procedures are extensively benefitted by the use of Digital Signature Certificates.

1.6 INGREDIENTS OF A DIGITAL SIGNATURE CERTIFICATE

The ingredients of a Digital Signature Certificate *inter alia* include the following details:

(a) The name of the individual owing the digital signature certificate
(b) The public key held by the owner of the digital signature certificate
(c) The date of expiry associated with the public key held by the owner
(d) The name of the certifying authority issuing the digital signature certificate
(e) The serial number associated with the digital signature certificate
(f) The digital signature of the owner/user of the digital signature certificate

1.7 SUBSCRIBER'S OBLIGATIONS

Besides imposing statutory obligations on the Certifying Authorities issuing Digital Signatures Certificates, the provisions of the Information Technology Act, 2000 also impose certain obligations on the subscribers applying for the Digital Signature Certificates. Such obligations are as follows:

i) Providing correct information devoid of errors, omissions, misrepresentations etc. in the application for the Digital Signature Certificate.
ii) Accepting the Digital Signature Certificate as generated by the Certifying Authority if all the information contained in the Digital Signature Certificate applied are validated to be true.
iii) In the event there are any changes required to be made in the Digital Signature Certificate of the subscriber to prevent the certificate from being misleading, the same shall be correctly provided by the subscriber forthwith after such change takes place.
iv) Ensuring the protection of the private key in a secure medium.

v) Ensuring that the certificate is terminated in case the information contained in such certificate is inaccurate and misleading.

The Act lists down the duties of subscribers in sections 40, 40A, 41 and 42 in the following manner.[90]

Section 40 *– Generating Key Pair – Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.*

Section 40A *– Duties of subscriber of Electronic Signature Certificate – In respect of Electronic Signature Certificate, the subscriber shall perform such duties as may be prescribed.*

Section 41 *– Acceptance of Digital Signature Certificate – (1) The subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate –*

(a) to one or more persons;

(b) in a repository;

or otherwise demonstrates his approval of the Digital Signature Certificate in any manner;

(2) By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

[90]Ross Anderson and Eli Biham (1996). Tiger: A Fast New Hash Function, Fast Software Encryption, Third International Workshop Proceedings, Springer-Verlag, pp. 89—97

1.8 DISADVANTAGES OF DIGITAL SIGNATURE CERTIFICATES

In spite of the extensive advantages associated with Digital Signature Certificates, there are a handful of disadvantages that arise from the issuance, use and implementation of Digital Signature Certificates, such as follows:

(a) Financial disadvantage: Certifying Authorities that issue Digital Signature Certificates require a monthly subscription from the applicant of such certificate. Such monthly subscription and the hefty costs involved therewith could become a liability on the entity or individual applying for the Digital Signature Certificate.[91]

(b) Equipment Cost: Electronic signatures that are required to be read by upgraded technology which warrantsthe extensive investment. Such expenses might become too heavy for certain applicants of Digital Signature Certificate.

(c) Deterrence on Clients: Application for and implementation of Digital Signature Certificates involve the use of certain applications and advanced forms of technology. Since the system of issuance and use of Digital Signature Certificate involve an extensive understanding of sophisticated technology and functioning of equipment, some clients might face trouble using Digital Signature Certificate, which could in turn cause deterrence towards using Digital Signature Certificates.[92]

1.9 LET'S SUM UP

In this chapter, we have studied the concept of digital signature certificate along with the types and classes. Furthermore, we also studied about how certifying authority issues the certificate and the obligations of the subscriber. Finally, we have ended our discussion with the advantages

[91]CCA. (2009). Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, CCA India, version 2.4 updated on 14th June 2011
<http://cca.gov.in/rw/resource/dsc _guidelines_r2_4.pdf>
[92] IT ACT (2000), The Information Technology Act, 2000, Government of India
<http://www.mit.gov.in/sites/ upload_files/dit/files/downloads/itact2000/itbill2000.pdf>

and disadvantages of digital signature certificate along with the statutory provisions pertaining to it.

1.10 FURTHER READING

- http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf
- Roy, Dr.Abhishek&Karforma, Sunil. (2012). A survey on digital signatures and its applications. JCIT. 3. 45-69.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is a Digital Signature Certificate?**

A. A Digital Signature Certificate is the electronic equivalent of physical form of certificates that can act as proof of identity for individuals, or sign documents digitally.

2. **Who issues Digital Signature Certificates?**

A. An individual or an entity authorised to grant Digital Signature Certificates as per section 24 of the Information Technology Act, 2000.

3. **What are the classes of Digital Signature Certificates?**

A. Digital Signature Certificates can be classified into three classes – Class 1, Class 2 and Class 3. Class 1 certificates are issued to users to authenticate their details such as name, email address etc. Class 2 certificates verify the identity of a person against a trusted, pre-verified database. Class 3 certificates involve the appearance of the applicant before the certifying authority for proving the identity.

4. **How long do Digital Signature Certificates remain valid?**

A. Digital Signature Certificates can stay valid for a minimum of one year to a maximum of three years.

5. **What is the legal status associated with Digital Signature Certificates?**

A. Digital Signature Certificates are admissible in courts of law in accordance with the provisions of the Information Technology Act, 2000.

1.12 ACTIVITY

Describe the issues and challenges associated with addressing identity theft in cyberspace in light of digital signature certificates and their applicability. (800 words)

Unit 3: Regulation and Responsibilitie Certifying Authorities and Controller Certifying Authorities

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Regulation of Certifying Authorities

1.4 Statutory Responsibilities of Certifying Authorities

1.5 Statutory Powers of Controllers of Certifying Authorities

1.6 Conclusion

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Role of Certifying Authorities and Controller of Certifying Authorities
- Regulation of Certifying Authorities and Controller of Certifying Authorities
- Powers of Controllers of Certifying Authorities

1.2 INTRODUCTION

As per the existing laws in our country, Digital Signature Certificates are issued by Certifying Authorities in accordance with the provisions of the Information Technology Act, 2000. Certifying Authorities, therefore, have a very significant role to serve in, which is in turn backed by statutory obligations and responsibilities. Before a Certifying Authority starts issuing Digital Signature Certificates, it is required to receive a license from the controller of certifying authorities. Certifying Authorities, in essence, play a twin role by issuing Digital Signature Certificates to subscribers in one hand and identifying with and authenticating such subscribers

on the other. Given that Certifying Authorities play a very crucial role in the process of generation of Digital Signature Certificates, it is also important to regulate the activities of such Certifying Authorities.

1.3 REGULATION OF CERTIFYING AUTHORITIES

The provisions of the Information Technology Act, 2000 acknowledge an authority superior to Certifying Authorities and refers to the same as the 'Controller of Certifying Authorities'. Chapter VI of the Information Technology Act, 2000 lay down provisions that elaborate upon means and ways for the Controller of Certifying Authorities to regulate Certifying Authorities. Guidelines that are to be followed by Certifying Authorities have also been laid down in ***the Information Technology (Certifying Authorities) Rules, 2000*** and ***the InformationTechnology (Certifying Authorities) Regulations, 2001.***[93]

As per the legal regulations and obligations of the Certifying Authorities, and the powers conferred to them in accordance with the law of the land, the nature of such entity should rather be an administrative authority than being a quasi-judicial body. Accordingly, ***Section 17 of The Information Technology Act, 2000*** lays down those requisites associated with the appointment of the Controller of Certifying authorities and other offices. By virtue thereof, the central government has the authority to appoint the Controller of Certifying Authority which in turn could have three functional departments such as (a) Technology, (b) Finance and Legal and (c) Investigation. Each department is to have a deputy controller and assistant controllers to oversee the smooth functioning of the entity.[94]

As a part of regulating the functions of the Certifying Authorities, the Controller of Certifying Authorities is required to perform certain functions as laid down under section 18 of the Information Technology Act, 2000, which inter alia include:

(i) Exercising supervision over the activities of the Certifying Authorities: As has been stipulated under Rule 31 of the Information Technology (Certifying Authority) Rules, 2000, the Certifying Authority shall be required to conduct half-yearly or quarterly

[93] Information Technology Act, 2000
[94] The Cyber Regulations Tribunal (Procedure) Rules, 2000

audits and submit such reports to the Controller of Certifying Authorities within four (4) weeks from the date of completion of such audit. The essence of this provision lies in the fact that as a Certifying Authority, as a licensee, is required to fulfil such conditions as are stipulated by the Controller of Certifying Authorities.

(ii) Certifying public keys of Certifying Authorities: The Root Certifying Authority of India (RCAI) has been established by the Controller of Certifying Authorities to certify public keys of the Certifying authorities in the country, as a result of which, the RCAI shall be *inter alia* responsible for digitally signing public keys of licensed Certifying Authorities; issuing licenses etc.

(iii) Laying down standards to be maintained by the Certifying Authorities: Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 lays down the standards that are to be considered for the functioning of Certifying Authorities.

(iv) Specifying the qualifications and experience which employees and Certifying Authorities should possess: This provision mandates that a system administrator be appointed to oversee that the protective security measure associated with the system are entirely functional and that a network administrator is appointed as an individual responsible for ensuring that the operations are executed properly.

(v) Specifying conditions subject to which the Certifying Authorities conduct their business.

(vi) Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an Electronic Signature Certificate and the public key.[95]

(vii) Specifying the form and content of an Electronic Signature Certificate and the key.

(viii) Specifying the form and manner in which accounts shall be maintained by Certifying Authorities: as per regulation 3 (vi) of the Information Technology (Certifying Authorities) Regulations, 2001, Certifying Authorities are required to comply with the financial mandates and parameters as issued under the Act during the period when the license will stay valid.

(ix) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them: This is to be complied with in sync with Rule 31 and

[95] Gupta, Apar, Commentary on Information Technology Act, 2000, LexisNexis ButterworthsWadhwaNagpur Publication, Ed. 2, 2011

32 of the Information Technology (Certifying Authorities) Rules, 2000, which in turn lay down the terms of regulating audit and auditor's relationship with Certifying Authorities.

(x) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of systems: As per Rule 19(2) of the Information Technology (Certifying Authorities) Rules, 2000, security guidelines have been laid down to ensure that integrity, confidentiality and availability of data, services and systems of Certifying Authorities are maintained.

(xi) Specifying the manner in which the Certifying Authorities shall conduct dealings with the subscribers: As per regulation 3 of the Information Technology (Certifying Authorities) Rules, 2001, a Certifying Authority is required to use methods which the Controller of Certifying Authorities has approved for the purposes of verifying a subscriber's identity before issuing or renewing any public key.[96]

(xii) Resolving ant conflict of interests between the Certifying Authorities and subscribers: As per Rule 12 of the Information Technology (Certifying Authorities) Rules, 2000, disputes arising between Certifying authorities and subscribers shall be referred for resolution to the Controller of Certifying authorities through arbitration or any other mode of resolution.

(xiii) Laying down the duties of the Certifying Authorities.

(xiv) Maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public: Rule 22 of the Information Technology (Certifying Authorities) Rules, 2000 makes reference to the database of Certifying Authorities, thereby stating that the Controller shall be required to maintain a database for the disclosure record.

1.4 STATUTORY RESPONSIBILITIES OF CERTIFYING AUTHORITIES

The statutory responsibilities and obligations that Certifying Authorities are legally required to abide by have been laid down in the provisions of the Information Technology Act, 2000:

(a) ***Section 35*** – Certifying Authority to issue Electronic Signature Certificate: This provision addresses that any person who wants to acquire a Digital Signature Certificate

[96] Henery Chan, Raymond Lee, Thoram Dillon, Elizabeth Chang, E-Commerce; Fundamentals and Applications, Wiely IndiaPvt. Ltd (India), Reprint 2008

can file an application addressing the Certifying Authority requesting the issuance of the certificate in the prescribed manner, coupled with the payment of the requisite application fee which shall not exceed Rs. 25,000/- (Rupees Twenty-Five Thousand only). The provision further mandates for the application to be accompanied by a 'certification practice statement' or any other statement specifying the necessary particulars, in absence of the former. In approval of the application submitted, a Digital Signature Certificate may be issued by the Certifying Authority after making the necessary enquiries, or the application may be rejected with relevant reasons recorded in writing after providing the applicant with an opportunity of showing cause against such rejection of the application.[97]

(b) ***Section 36*** – Representations upon issuance of Digital Signature Certificate: The provision lists down the requisites that a Certifying Authority is legally required to ensure while issuing a Digital Signature Certificate. It is mandated as per the section that –

i. The provisions of the Act, as well as the rules and regulations associated with it, have been complied with while the issuance of the Digital Signature Certificate;
ii. The Digital Signature Certificate has been published or otherwise made available to the applicant and that the applicant has acknowledged the same;
iii. The applicant holds the private key and its corresponding public key as listed in the Digital Signature Certificate;
iv. The applicant holds the private key that creates a digital signature;
v. The public key as listed in the Digital Signature Certificate is capable of verifying the digital signature affixed by the private key that the applicant holds;
vi. The public key and the private key held by the applicant together form a valid and functioning key pair;
vii. The Digital Signature Certificate only contains information that is accurate;
viii. No material fact exists that is potentially capable of adversely affecting the reliability of the aforementioned conditions.[98]

[97] Sharma, Vakul, Information Technology and Practice, Universal Law Publication, 2008
[98] Indira Carr, India joins the cyber-race: Information Technology Act 2000, Int. TJs 2000, 6(4), 122-130, (2000)

(c) ***Section 37*** – Suspension of Digital Signature Certificate: this provision of the act endows upon the Certifying Authority issuing the Digital Signature Certificate the power to suspend such Digital Signature Certificate granted on certain grounds; such as, upon receipt of a request of such suspension of certificate from the person listed as the subscriber in the Digital Signature Certificate or any other person authorised to act on his or her behalf; or in the event the Certifying Authority believes that the suspension of such Digital Signature Certificate shall be in the interest of the public at large. Furthermore, the provision further lays down that unless the subscriber has been given an opportunity of being heard with respect to such suspension of the Digital Signature Certificate, the certificate shall not be suspended for any longer than fifteen days. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such suspension of the Digital Signature Certificate.

(d) ***Section 38*** – Revocation of Digital Signature Certificate: This provision addresses instances that could cause the Certifying Authority issuing a Digital Signature Certificate to revoke it. The circumstances in which the Certifying Authority could so revoke a Digital Signature Certificate granted by itself are –

(i) The subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(ii) A person duly authorised by the subscriber of the Digital Signature Certificate making a request of revocation of the certificate granted;

(iii) Upon death or insolvency of the subscriber of the Digital Signature Certificate;

(iv) In instances wherein the subscriber of the Digital Signature Certificate is a firm or a company, the respective dissolution and winding up thereof;

(v) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that incorrect and erroneous information has been represented as material facts in the Digital Signature Certificate;

(vi) In the event the Certifying Authority issuing the Digital Signature Certificate is of the opinion that a material requirement associated with the issuance of the Digital Signature Certificate remains unfulfilled;

(vii) In the event, the Certifying Authority issuing the Digital Signature Certificate is of the opinion that the security system and/or the private key held by the Certifying Authority had been compromised so as to affect the reliability of the Digital Signature Certificate.

The provision, however, emphasises on how the Digital Signature Certificateis not to be revoked without giving its subscriber a reasonable opportunity of being heard. It further imposes on the Certifying Authority the obligation of communicating to the subscriber all information associated with such revocation of the Digital Signature Certificate.[99]

1.5 STATUTORY POWERS OF CONTROLLERS OF CERTIFYING AUTHORITIES

The Information Technology Act, 2000 lays down provisions to address the powers of the Controller of Certifying Authorities in a manner such as follows:

(i) ***Section 27*** – Power to delegate – As per the Act, the Controller shall have the power to authorize the deputy controller of Certifying Authorities, or any other office, in writing, to exercise the powers of the Controller in the same capacity. This provision of the Act is to be ideally read with section 17 thereof, which in turn lays down the organizational structure of the Controller and its team along with the Deputy Controllers, Assistant Controllers and other officers and employees. Nevertheless, in spite of such delegation made by the Controller, the quasi-judicial powers held by the Controller to resolve disputes, if any, between the Certifying Authorities and the subscribers, shall necessarily be retained with the Controller.

(ii) ***Section 28*** – Power to investigate contraventions- Any contravention of the provisions of the Act and/or rules and/or regulations can be taken up for investigation by the Controller or any officer authorized by the Controller. In such event of an investigation, the powers conferred on Income Tax authorities under chapter XIII of the Income Tax Act, 1961, shall apply on the Controller or any other officer authorized by the Controller for the purposes of this provision, however, in accordance with the limitations as laid down under that Act. This power as grated vide this provision is solely investigative in nature. This provision further signifies

[99]Vakul Sharma, Information technology: Law and Practice, Universal Law Publication, Ed. 2, 2008

that the Controller or any other officer authorised by him/her, shall be deemed to have the power to impound and retain in custody documents or books of accounts produced through search or seizure for such period of time that it may deem fit.

(iii)***Section 29*** – Access to computers and data – This provision grants to the Controller or any other person authorized by it broad powers to search and have access to any computer system, apparatus, data connected to such system, etc. solely based upon the reasonable cause to believe that a contravention of the Act or its provisions has been committed.

1.6 CONCLUSION

The provisions of the Information Technology Act, 2000 address the necessity of ensuring that the integrity associated with the system of acquiring and implementing digital signatures is maintained through the delegation of responsibilities amongst various statutory bodies such as Certifying Authorities, Controller of Certifying Authorities, etc. In a world which is going through a dramatic transition that envisages a sea of technological changes which might take extensive sophistication to tackle, it is of utmost importance to ensure that there is due regulation at every stage of action, and that requisite measures have been taken to address any mishap and/or contravention of the ideal provisions laid down as guidelines. In an age where digital signatures are replacing manual signatures, and digital signature certificates are gaining prominence; and public at large are slowly and steadily acknowledging the convenience associated with such change, it is essential that the government ensures that there is enough regulation in place to address instances wherein a misuse or misinterpretation of such nascent and modern technology could take place.[100] It is for this purpose that the Certifying Authorities have been statutorily established, and the Controller of Certifying Authorities have been laid down. Furthermore, the law of the land also ensures that there are specific guidelines established to address the functioning of such authoritative bodies, establish their hierarchy, carve out their responsibilities and powers and in turn create inter-linking of laws for better implementation of such provisions. It is therefore extremely important to learn about the responsibilities, functions and modes of regulating Certifying Authorities as well as Controllers of Certifying Authorities.

[100]VivekSood, Cyber Law Simlpified, Fourth Ed., 2008, Tata McGraw-Hill Publishing Company Ltd

1.7 LET'S SUM UP

In this chapter, we have studied who is a certifying authority along with the regulations and statutory powers under the Information Technology Act, 2000. Finally, we have ended the discussion with the powers given to the certifying authorities.

1.8 FURTHER READING

- http://www.commonlii.org/sg/journals/SGJlIntCompLaw/2003/9.pdf
- Regulation of Certifying Authorities - The Informational Tech. Act, 2008, B.Com, EDUREV.IN (2019), https://edurev.in/studytube/Regulation-of-Certifying-Authorities-The-Informati/74d7d226-f41e-4dfa-97e8-4a9b6bf40993_p?courseId=-1 (last visited Nov 19, 2019).
- Ikram, N. & A., Mahboob,. (2002). Regulatory Issues with Certification Authorities.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Who is a Controller of Certifying Authorities?**

A. A Controller of Certifying Authorities is the entity that supervises the functioning of the Certifying Authorities.

2. **What are the functions of the Controller of Certifying Authorities?**

A. The functions of the Controller of Certifying Authorities inter alia include supervising the functions of the Certifying Authorities, certifying public keys for Certifying Authorities, laying down standards to be maintained and followed by Certifying Authorities etc.

3. **What are the statutory powers of Controller of Certifying Authorities under the existing laws?**

A. The statutory powers of Controller of Certifying Authorities under the existing laws include the power to delegate, the power to investigate contravention of provisions of the act, access to computer data, etc.

4. Which provisions of the Act address the statutory responsibilities of certifying authorities?

A. The provisions of the Act address the statutory responsibilities of certifying authorities are sections 35, section 36, section 37 and section 38.

5. What are the sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities?

A. The sources of laws, rules and regulations that address the functioning and regulation of Certifying Authorities and Controller of Certifying Authorities are provisions of the Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and the Information Technology (Certifying Authorities) Regulations, 2001.

1.10 ACTIVITY

Under the IT Act 2000, what are the implications for 'Certifying Authorities'? (800-1000 words)

Unit 4: Addressing Offences: Penalties and Compensation

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Provisions applicable to Certifying Authorities and their Controller

1.4 Penalties in respect of damage to systems associated with cyberspace

1.5 Let's sum up

1.6 Further reading

1.7 Check your progress: Possible answers

1.8 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter you should be able to understand

- Concept of Offences in Cyber Laws
- Commission of Offenses owing to Acts and Omissions of the Controller
- Commission of Offenses owing to Acts and Omissions of the Controller of Certifying Authorities

1.2 INTRODUCTION

The interesting aspect relating to penalties associated with cyber laws is that the provisions addressing them are directed towards penalties towards damage to computer and computer systems as well as towards the process of adjudication. For example, while on one hand, the provisions of the Information Technology Act, 2000 address issues of breach of security or privacy, on the other, it also deals with acts of failing to protect data and privacy. Similarly, the provisions of the Act further address instances wherein the Controller of a Certifying Authority has acted in a manner that is in violation of the provisions of the Act, or had omitted performing

its duties and responsibilities so as to contravene the provisions of the Act. The provisions of the Act and the rules and regulations pertaining to penalties, compensation and adjudication hence have to be read in sync with the essence of cyber laws at large. The Act is governed by the principle ***"He who does not prevent a crime when he can, encourages it."***

1.3 PROVISIONS APPLICABLE TO CERTIFYING AUTHORITIES AND THEIR CONTROLLER

The Information Technology Act, 2000 lays down provisions that give the Controller of Certifying Authorities the power to direct certain necessary measures to be taken to ensure compliance with the provisions of the Act; and any violation by any individual of such direction or order as given by the Controller is deemed to constitute an offence under the Act.

Similarly, suppression of material facts and/or misrepresentation of facts from Certifying Authorities or their Controller for the purposes of obtaining a license or an electronic piece of document is an offence in accordance with the provisions of the Act.[101]

An elaborate understanding with respect to the aforementioned provisions are provided hereinbelow:

i) ***Section 68 – Power of controller to give directions*** *– (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.*[102]

This provision is in turn backed by the ***'Information Technology Security Guidelines'*** and the ***'Security Guidelines for Certifying Authorities'*** issued under the Information Technology (Certifying Authorities) Rules, 2000 which prescribe the security standards which are to be

[101] Offences & Penalties under the IT Act, 2000 <http://www.legalservicesindia.com/article/439/Offences-&-Penalties-under-the-IT-Act,-2000.html>

[102] The Information Technology Act, 2000, s 68(2)

observed by Certifying Authorities and endowing upon them the power to issue directions. While a general interpretation of the provision makes it is evident that the Controller has the power to Certifying Authorities and/or employees thereof, in essence such power can be further extended to apply on subscribers of a digital certificate as well, which can be inferred by a combined reading of ***section 68 with section 18(1) of the Information Technology Act, 2000,*** which states that the Controller shall expressly have the power to resolve any and all conflicts of interests and/or disputes between the subscriber and the respective Certifying Authorities.

Sub-section (2) of the provision goes on to establish that the offence committed by way of non-compliance of the order passed under sub-section (1) shall be a cognizable and non-bailable offence. Since section 27 of the Act allows a Controller to delegate its authorities and responsibilities to a Deputy Controller or an Assistant Controller; accordingly, a non-compliance of the Controller's order by such Deputy Controller or the Assistant Controller shall also fall within the ambit of section 68.

A combined reading of section 68 of the Act with sections 28 and 29 which in turn expressly grant to a Controller the power to investigate contraventions of the Act will clarify that the Certifying Authority has the responsibility to ensure that there is no contravention of the Act in the first place; and of at all the same is conducted by any entity and/or individual, then it will constitute as an offence.

ii) ***Section 71*** *– Penalty for misrepresentation – whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.*

In addition to the powers already endowed upon the Certifying Authorities and their Controller through ***section 25 and section 38 of the Act*** to suspend and revoke the license and digital signature certificates, this provision additionally bestows upon the Certifying Authority as well as its Controller the obligation to ensure that applicants who misrepresent information or suppress material information are brought within the ambit of criminal charges.

These two aforementioned provisions of the Act bring to the fore how the intention of the legislature was to address such instances in a criminal light wherein any entity, whether statutory

or otherwise, associated with electronic transactions and/or applications and/or involved any correspondence involving the cyberspace tries to misuse the relevant provisions of law and take advantage thereof.

1.4 PENALTIES IN RESPECT OF DAMAGE TO SYSTEMS ASSOCIATED WITH CYBERSPACE

The Information Technology Act, 2000 addresses instances of cyber contraventions through provisions that deal with penalties and/or compensation. Majorly section 43 to section 45 address the aforesaid and in turn list down variable penalties applicable to the respective offenders in accordance with the nature of offence committed.[103] A brief overview of the provisions is provided hereinbelow:

a) ***Section 43*** lists the various instances wherein there could be damage caused to computers or their systems or networks.
b) ***Section 43 A*** deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.
c) ***Section 44*** directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.
d) ***Section 45*** addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

Section 43 lays down that unauthorized access to computers, an attempt thereof or an assistance thereto are offences under the Act. The ambit of the clause states that such unauthorized access shall cover both physical and virtual access to the computer or its system or network. Such access may be established inter alia if the computer is found to have performed a function as a result of such access. The provision further addresses unauthorized infringement of digital data stored in such computer or its network inter alia through downloading, copying, extracting etc. For the purposes of this provision, downloading, copying and extracting may be differentiated in the following manner –

[103]Penalties and Adjudication in IT ACT 2000
<https://www.pathlegal.in/Penalties-and-Adjudication-in-IT-ACT-2000-blog-1831947>

Downloading	***Copying***	***Extracting***
A file containing digital content being retrieved from a remote computer or network.	A file containing digital content being retrieved from a remote computer or network and then being saved in a storage medium.	A file containing digital content being retrieved from a remote computer or network and then being selectively extracted.

The provision further addresses instances wherein contaminants may be introduced within the computer or its network, and any other attempts that can potentially be made to contaminate data contained in a computer or its network, or destroy, steal, delete, alter the same. Such unauthorized damage to the contents contained in the computer or its computer could be both physical as well as virtual. For the purposes of this provision, physical unauthorized damage and virtual unauthorized damage may be differentiated in the following manner:[104]

Physical Unauthorized Damage	***Virtual Unauthorized Damage***
This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner.	This could imply changing the configuration of the original software or the original hardware of any computer, computer system or computer network and/or destroying, deleting, altering, modifying in any manner whatsoever the binary files (which shall include but nit be limited to data or other computer programs) available in a computer, computer system or computer network in an unauthorized manner by way of being remotely connected to such device or network using

[104]Damages or Compensation under IT Act 2000 in India <https://cybercrimelawyer.wordpress.com/2018/04/12/damages-or-compensation-under-it-act-2000-in-india/>

	satellite and/or terrestrial waves and/or microwaves and/or other communication media.

Disruption of a computer or its system or network or denial of access thereto is also considered an offence under this provision. A summary of the sub sections of Section 43 of the Act along with the scope thereof is provided hereunder:

Information Technology Act, 2000	***Scope of Section 43***
Section 43 – Penalty and compensation for damage to computer, computer system, etc. : If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network[105]	The provision majorly addresses all the probable contraventions arising out of unauthorized access to computer, computer system or computer network.
(a) Accesses or secures access to such computer, computer system or computer network or computer resources;	Instances of cracking, hacking, data theft, software piracy etc. will be addressed as a part hereof.
(b) Downloads, copies or extracts data, computer database or information from such computer, computer system or computer network, including information or data stored or held in any removable storage medium;	Instances of digital copying, data theft, violation of privacy will get addressed.

[105]ISACA *State of Cybersecurity: Implications for 2015*
<http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf>

(c) Introduces or causes to be introduced any contaminant or computer virus into any computer, computer system or computer network;	Instances of deletion, alteration, destruction, modification of any data stored in a computer would get addressed.
(d) Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;	Instances related to forgery, online fraud, violation of privacy would get addressed.
(e) Disrupts or causes disruption of any computer, computer system or computer network;	Instances such as spamming attacks, denial of service etc. will get addressed.
(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;	Issues related to system interference, misuse of computer devices etc. get covered hereunder.
(g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of the Act, rules or regulations made thereunder	Instances of illegal access, misuse of computer devices etc. get covered hereunder.

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network	Online fraud, phishing, identify theft etc. are the instances that could be addressed through this provision.
(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means	Cracking, hacking, data theft, interference into and loss of data, online frauds and forgeries etc. are instances to get covered under this sub-section.
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage	This sub-section could cover instances related to violations of computer programs and software, theft, piracy etc.

Section 43A addresses all instances of violation of the Act arising and accruing from negligence on part of the data processor or controller. This provision is proactive in nature and aims at protecting personal data and information. The provision further identifies body corporates as 'data processors and controllers for possessing, dealing with and/or handling sensitive data, as the case may be. As opposed to the provisions of section 43, section 43A is specifically addressed towards body corporates. The provision further goes on to warrant that in the event

there is a violation of such sensitive and/or personal data invoking the contents of this section, such violation shall entail payment of compensation.[106]

Section 44 of the Act addresses a range of offences thereby imposing a range of penalties on the contravener of such provision in the following manner:

Section 44	***Authority***	***Applicability***	***Penalty Amount***
Clause (a)	Controller or the Certifying Authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure.
Clause (b)	Controller, any government agency, statutory authority	Subscribers, Auditors, Computer Resource Incharge, etc.	Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure.
Clause (c)	Controller, any government agency, statutory authority	Certifying Authority, Computer Resource Incharge, etc.	Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure

Section 45 is in essence effective against all contraventions for which no separate penalty has been provided.[107] Therefore, unless an offence is carefully judged and categorized under sections

[106]National Institute of Standards Technology*Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.*
<http://dx.doi.org/10.6028/NIST.SP.800-30r1>

43, 43A or 44, it will by default invoke section 45. A summary of the penalties associated with the provisions is provided hereunder:[108]

Contraventions under the Act	***Penalty Amount***
Section 43 – Penalty and compensation for damage to computers and computer systems	i) Less than Rs. 5,00,00,000/- (Rupees Five Crores only) before the adjudicating officer ii) More than Rs. 5,00,00,000/- (Rupees Five Crores only) before the competent civil court.
Section 44 – Penalty for failure to furnish information, return, etc.	i) Less than Rs. 1,50,000/- (Rupees One Lakh and Fifty Thousand only) for each such failure. ii) Not exceeding Rs. 5,000/- (Rupees Five Thousand only) for each day during such continuing failure. iii) Not exceeding Rs. 10,000/- (Rupees Ten Thousand only) for each day during such continuing failure
Section 45 – Residuary Penalty	Not exceeding Rs. 25,000/- (Rupees Twenty Five Thousand only).

1.5 LET'S SUM UP

In this chapter, we have studied the concept of offences in cyber law along with those provisions that are applicable to Certifying Authorities and their Controller. Finally, we have ended the discussion with the penalties in respect of damage to systems associated with cyberspace.

[107] <http://www.meity.gov.in/content/information-technology-act-2000>
[108] The Gazette of India, The Information and Technology Act, 2000, no. 27 of 2000, The Ministry of Law, Justice and Company Affairs, Part II, New Delhi

1.6 FURTHER READING

- Zenithresearch.org.in (2019), http://zenithresearch.org.in/images/stories/pdf/2012/May/ZIJBEMR/13_ZIBEMR_VOL2_ISSUE5_MAY2012.pdf (last visited Nov 22, 2019).
- Indian - Computer Emergency Response Team, Cert-in.org.in (2019), https://www.cert-in.org.in (last visited Nov 22, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the powers of the controller to give directions?**

As per Section 68 of the Act, The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder. (2) Any person who intentionally and knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction or imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or both.

2. **What is the punishment for misrepresentation?**

As per Section 71 of the Act, whoever makes any misrepresentation to or suppresses any material fact from the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate as the case may be shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both.

3. **Give a brief overview of the provisions with respect to damages to systems associated with cyberspace?**

a) Section 43 lists the various instances wherein there could be damage caused to computers or their systems or networks.

b) Section 43 A deals with an act of failure to protect sensitive data and entails payment of damages by the contravener by way of compensation.

c) Section 44 directs for a penalty to be provided for failure in furnishing information by any person who is required by the Act to provide such information or file any return or maintain books of accounts.

d) Section 45 addresses residuary penalty towards those who violates the rules and regulations made in association with the Act and for the specific contravention of which no penalty has separately been provided.

1.7 ACTIVITY

Discuss the powers of the investigating machinery under the Information Technology Act, 2000. (1000 words)

Block 3
Laws related to E-Service Delivery and Service Providers

Unit 1: E-Services Delivery Laws in India

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Electronic Delivery of Services Bill introduced in Parliament of India

1.4 Duty of the Competent Authority to notify the list of public services to be delivered through electronic mode

1.5 Functions and Powers of Director of Electronic Service Delivery

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- E-Service Delivery Concept in India
- Purpose of the Electronic Delivery of Services Bill (EDS), 2011
- Functions and Powers of Director of Electronic Service Delivery.

1.2 INTRODUCTION

Government of India has been at the forefront of using technology in different aspects of governance, be it satellite-based communication in the 1980s or use of electronic messaging much before the origin of the internet in the country or even the use of video conference for monitoring of government programme and schemes across the country. National Informatics Centre, an attached office of Ministry of Electronics & IT has been closely working with the government in provisioning state-of-the-art infrastructure in the form of nationwide network

(NICNET), data centres and video conferencing facilities to name a few. Digital technologies are vital for the inclusive growth for a country like India, which is at the peak of its demographic dividend.

The story of India's digital transformation is one of an ***Information and Communications Technology (ICT)*** led development by use of technology that is affordable, inclusive and transformative. By ensuring digital access, digital inclusion and digital empowerment, the ***'Digital India'*** programme[109] have brought digital technologies a positive change towards good governance that is easy, economical, transparent and efficient in governance. Digital delivery of services to citizens forms the driving force for the next generation growth and knowledge-based economy. India is now poised for the next phase of growth - the creation of tremendous economic value and empowerment for citizens as a new digital application sector.

Digital India has given boost to entrepreneurship and has enhanced access to health, education and public utilities. It has led India to revolutionize governance by delivering speedy and transparent services to citizens, ensuring their participation and empowering them with the conducive environment to connect and grow.

1.3 ELECTRONIC DELIVERY OF SERVICES BILL INTRODUCED IN PARLIAMENT OF INDIA

The Electronic Delivery of Services Bill (EDS), 2011, aimed at bringing transparency in public dealings and checking corruption, was tabled in Parliament. The Bill seeks to reduce the interface between public and government officials to save time and costs as people will get access to documents like driving license and other permits online. The EDS Bill allows for ***"delivery of public services through electronic mode including the receipt of forms and applications, issue or grant of license, permit, certificate, sanction or approval and the receipt and payment of money."*** Centre, as well as the states, will have to deliver the said public services electronically within five years of the commencement of the Act. The period may be extended for a further period of up to three years in consultation with the Central Commission or the State Commission, the Bill said.

[109]'E-Governance In India : Empowering Citizens - Current Affair Article For UPSC, IAS, Civil Services And State PCS Examinations | Dhyeya IAS Best Coaching For UPSC, IAS,Civil Services, State PSC/PCS Exam' (*Dhyeyaias.com*, 2020) <https://www.dhyeyaias.com/current-affairs/perfect-7-magazine/e-governance-in-india>

"Every competent authority shall publish within 180 days from the commencement of the Act, the list of all public services to be delivered through electronic mode," it added. The Bill requires each Ministry or Department to identify the basket of citizen-centric services to be delivered through the electronic means along with the delivery channels, with stipulated timelines and service levels for each service. An aggrieved person may file a complaint under the Grievance RedressalMechanism, the Bill imposes penalties of up to Rs 5,000 for officials in case they fail to adhere to the norms.

In case of persistent default, the penalty may extend up to Rs20,000, the Bill said The Bill also envisages setting up a Central Electronic Service Delivery Commission and a State Electronic Service Delivery Commission to monitor the implementation of the Act on a regular basis. Any person aggrieved by the order of the Grievance Redressal Mechanism may make a representation to the Central Electronic Service Delivery Commission or the State Commission as the case maybe, the Bill said.

A bill to provide for delivery of public services by the Government to all persons by electronic mode to enhance transparency, efficiency, accountability, accessibility and reliability in the delivery of such services, and including matters connected therewith or incidental thereto. WHEREAS it is considered necessary to provide a legal framework to promote efficient electronic delivery of government services, 2011.[110]

1.4 DUTY OF THE COMPETENT AUTHORITY TO NOTIFY THE LIST OF PUBLIC SERVICES TO BE DELIVERED THROUGH ELECTRONIC MODE

(1) Every Competent Authority shall notify within a period of thirty days from the coming into force of these rules-

(a) The public services of the department, agency or body, which can be delivered through electronic mode;

[110]THE ELECTRONIC SERVICE DELIVERY BILL, 2011
<https://www.prsindia.org/uploads/media/draft/Draft%20Electronic%20Service%20Delivery%20Bill-2011.pdf>

(b) The date by which each such service shall be made available through electronic mode,

(c) Lay down norms for efficiency, quality and accuracy in the form of service levels; and

(d) The designated officers for delivery of each such service through electronic mode.

(2) Notwithstanding anything stated above, all public services shall be delivered in electronic mode within 5 years from the commencement of this Bill; Provided that this period may, for reasons to be recorded, be extended for a further period not exceeding 3 years by the appropriate Government; Provided further that if it is not feasible to render a public service through electronic mode, then the appropriate government shall issue a notification to that effect.

(3) The competent authority, while introducing electronic services, shall ensure that

a) The processes and forms relating to such services are simplified initially and periodically thereafter; and

b) Assisted access to such electronic services is also made available.

(4) The Central Government may, from time to time, prescribe electronic governance standards as may be necessary for ensuring interoperability and security.[111]

1.5 FUNCTIONS AND POWERS OF DIRECTOR OF ELECTRONIC SERVICE DELIVERY

The Director of Electronic Service Delivery shall discharge the following functions and powers, namely:-

a. To authorise, suspend or terminate the services of the Authorized Service Providers;

[111](Environment.delhigovt.nic.in, 2020) <http://environment.delhigovt.nic.in/wps/wcm/connect/29bf44804dd72a98a833ec8291a3c3a2/ESD+Rules.pdf?MOD=AJPERES&lmod=-1976042643>

b. To determine norms relating to the selection of authorised agents by the authorised Service Providers and authorised agents;[112]
c. To determine functions, responsibilities and liabilities of authorised Service Providers and authorised agents;
d. To determine norms on the service levels to be complied with by the authorised Service Providers and authorised agents;
e. To determine service charges be charged by the authorised Service Providers and authorised agents for providing e-services;
f. To determine terms and conditions relating to the authorisation, suspension or termination of the services of the authorised Service Providers and authorised agents; and
g. To make alternative arrangements for delivery of e-services, in case of such suspension or termination of services of authorised Service Providers and authorised agents.

- Director of Electronics Service delivery may delegate any of his power to any official of Government of NCT of Delhi or Autonomous Body/Local Body of Government of NCT of Delhi through an administrative order.

- ***Authorised Service Providers for Electronic Service Delivery***- The Authorised Service Provider shall provide the notified public services electronically to the users in conformity with these rules, by establishing appropriate delivery infrastructure and a network of authorised agents, as determined by the Director of Electronic Service Delivery.

- ***Appointment of authorised agents by the authorised Service Provider***-
  The authorised Service Provider may appoint such number of authorised Agents, as may be required to deliver the services electronically to fulfil the norms of efficiency, quality and accuracy laid down by the Competent Authority.[113]

[112] Das, Sudhir Chandra. (2012). E-Governance Mechanism in India: Experiences from Selected E-Governance Projects. Mirror: Peer Referred Bi-annual Research Journal of Commerce, Management and Social Science, Kerala INDIA II 166-177

- The authorised Service Provider shall ensure that he as well as all the authorised agents obtain Digital Signature Certificates before they commence operations for delivery of public service electronically.

- The authorised Service Provider may also impart appropriate training to the authorised agent to impart them the skills required to deliver the electronic services efficiently and in an error-free manner.[114]

- ***Commencement of operations by Authorised Service Provider***-
  The Authorised Service Provider shall commence its commercial operation for Electronic Service Delivery only after –

  - He has confirmed in writing or through e-mail duly signed by digital signature to the Director of Electronic Service Delivery with respect to the adoption of procedures and standards specified under these rules; and
  - He has installed facilities and infrastructure needed for efficient delivery of electronic services and in an error-free manner in terms of norms laid down by the Director of Electronic Service Delivery and confirm the same in writing or through email duly signed by digital signature to the Director of Electronic Service Delivery.

- ***Authorised Service Provider to collect service charge*** - (1) The application for an eservice submitted by a user to an authorised Service Provider or an authorised agent shall be accompanied by such service charge as may be determined by the Director of Electronic Service Delivery which is payable in cash to the authorised Service Provider, at the time of making the application.[115]

---

[113]Alanezi, M A, Kamil, A and Basri, S (2010), "A proposed instrument dimensions for measuring e-government service quality", International Journal of u- and e-Service, Science and Technology, Vol 3 No 4, pp 1-17

[114] Bhattacharya, Debjani& Gupta, MP (2012) E-service quality model for Indian government portals: Citizens' perspective. Journal of Enterprise Information Management

[115] Carter, L. and Be´langer, F (2005), "The utilization of e-government services: citizen trust, innovation and acceptance factors", Information Systems Journal, Vol 15, pp 5-25

- The Director of Electronic Service Delivery may determine service charges by notification for e-services.
- The service charges may be different for different e-services such as, -
    - The status enquiry;
    - print-outs related to e-services;
    - The scanning of documents related to e-services;
    - The acknowledgement receipt; and
    - Any other e-service.
- The service charge shall not include any duly authorized taxes, charges, dues or any other moneys due in respect of service payable by any person to the Competent Authority concerned that are otherwise payable under the respective Act, Rule, Regulation or order of the Government when making an application to the concerned Competent Authority.
- ***The fee to be collected by the service provider***-
    a. Any fee or duly authorized taxes, charges, dues or any other money due in respect of a service payable by any person to the Competent Authority concerned that are otherwise payable under the respective act rule, regulation or order of the government when making an application to the concerned Competent Authority, shall also be collected by the authorised Service Provider or the authorized agent as the case may be, except for those payments that are ordinarily required to be made in the form of court fee stamps or treasury challans.

    b. The fee collected by the authorised Service Provider or the authorised agent shall be remitted with the Government treasury as may be determined by the Director of Electronic Service Delivery by the authorised Service Provider or the authorised agent as the case may be, in its entirety.
- ***Remittance or service charge and fee by the service provider***-

  Out of the service charge collected by the authorised Service Provider or the authorised agent for an e-service, a percentage of the service charge as may be determined from time to time by the Director of Electronics Delivery may be apportioned to the Government.

- The share of the Government out of the service charge so collected shall be remitted by the Authorised Service Provider or the authorised agent to Government treasury as may be determined by the Director of Electronic Service Delivery.[116]
- ***Presumption with regard to service charge paid to service provide and other conditions of obtaining e-services***- (1) Where any person pays a service charge to an authorised Service Provider or an authorised agent in respect of any notified e-service, the print-out or the electronic prompt acknowledging the payment in the relevant form and manner as may be determined by the Director of Electronic Service Delivery and provided to such person by the authorised Service Provider or authorised agent shall normally be taken as proof of such payment and it shall be presumed that in normal circumstances the dues or claims, for which the acknowledgement is purportedly issued, have been satisfied to that extent. (2) The payment of service charges to the authorised Service Provider or the authorised agent shall by no means create any right or title, temporary or permanent in nature in favour of a person concerned regarding obtaining the notified e-services. (3) Mere payment does not necessarily ensure the delivery of services if all conditions associated with the delivery of the service are not met fully at the time of making payment to the authorised Service Provider or the authorised agent.[117]
- ***Receipt or payment of money by or in favour of Government adopting the system of Electronic Service Delivery***-

  The receipt or payment of money by or in favour of Government adopting the system of Electronic Service Delivery shall be deemed to be a receipt or payment effected in compliance with the Financial Code and Treasury Code of the Government.[118]
- ***Filing of form, application or any other document***-

  Any form, application or any other document referred to in clause (a) of sub-section (1) of section 6 of the Act may be filed with any office, authority, body, agency or authorised Service Provider authorised by the Government of National Capital Territory of Delhi using the application software specified by it.

[116]Chawla Rajeev and MukerjiAnirban (2007), E-Governeance Initiatives of Karnataka", Yojana, Vol 51, pp 26-29
[117]Heeks, Richard (1999), "I-Development, not E-Development", Journal of International Development, Vol 14(1), pp1-11
[118] Holmes, D (2001), E-Gov: E-Business Strategies for Government, Nicholas Brealey, London

(2) The office, authority, agency or authorised Service Provider referred to in sub-clause (1) shall, while developing such software, take into account the following features of the electronic record, namely:- (a) lifetime; (b) preservability; (c) accessibility; (d) readability; (e) comprehensibility in respect of linked information; (f) evidentiary value in terms of authenticity and integrity; (g) controlled destructibility; and (h) augment ability.

Issue or grant of any license, permit, sanction or approval-

- Any license, permit, sanction or approval referred to in clause (b) of sub-section (1) of section 6 of the Act may be issued or granted by using the application software specified under rule 15.
- The license, permit, certificate, sanction or approval so issued shall be in the form prescribed in the respective Act, rule, regulation or order and shall contain the name and designation of the signing authority who had digitally signed and approved the electronic record along with the date and time of the creation of such record.
- ***Creation or repository of digitally signed electronic records***- (1) The Competent Authority may, as soon as, after the coming into effect of these rules create, establish and maintain a repository and database of digitally signed electronic records together with the associated application software and workflow to enable authorised Service Provider or the authorised agents to access such licenses, permits, certificates, sanctions or approvals, as the case may be, and deliver them to the user.[119]
- The relevant security procedures, as specified by the Government, shall be followed by such Competent Authorities, in respect of the electronic data, information, applications, repository of digitally signed electronic records and information technology assets under their respective control.
- ***Procedure for making changes in a repository of digitally signed electronic records*** -
    a) Any Competent Authority or any signing authority, either suomotu, or on an application by an interested party, may make or order to make an appropriate change in a repository of digitally signed electronic records, after following the procedure prescribed in the respective Act, rule, regulation or order.

[119]Kochhar Sameer and Dhanjal (2005), "E-Governance Report Card", Yojana, Vol 49, pp 60-69

b) Any such authority shall have privileges for making or ordering changes only in respect of the electronic records pertaining to its own jurisdiction.

1.6 LET'S SUM UP

In this chapter, we have studied the meaning of electronic delivery and the duties of competent authority to notify the list of public services to be delivered through electronic mode. We also discussed the powers and functions of the director of electronic service delivery. Finally, we have ended the discussion with the electronic delivery of services bill introduced in the Parliament of India in 2011.

1.7 FURTHER READING

- Adb.org (2019), https://www.adb.org/sites/default/files/publication/467826/adbi-wp890.pdf (last visited Nov 19, 2019).
- Nazir, Mohsin&Wani, Sani&Arif, Tasleem. (2014). Current Scenario of the e-Governance Related Initiatives in India.
- Isec.ac.in (2019), http://www.isec.ac.in/WP%20-%20165.pdf (last visited Nov 19, 2019).
- https://www.nisg.org/files/documents/D01010001.pdf

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the aim of Electronic Delivery of Services Bill (EDS), 2011?**

A. The aim of Electronic Delivery of Services Bill (EDS), 2011 is aimed at bringing transparency in public dealings and checking corruption in public dealing. The EDS Bill allows for "delivery of public services through electronic mode including the receipt of forms and applications, issue or grant of license, permit, certificate, sanction or approval and the receipt and payment of money.

2. What are the main Functions and Powers of Director of Electronic Service Delivery?

A. To authorise, suspend or terminate the services of the Authorized Service Providers; To determine norms relating to the selection of authorised agents by the authorised Service Providers and authorised agents; To determine functions, responsibilities and liabilities of authorised Service Providers and authorised agents; To determine norms on the service levels to be complied with by the authorised Service Providers and authorised agents; To determine service charges to be charged by the authorised Service Providers and authorised agents for providing e-services; To determine terms and conditions relating to the authorisation, suspension or termination of the services of the authorised Service Providers and authorised agents; and To make a alternative arrangements for delivery of e-services, in case of such suspension or termination of services of authorised Service Providers and authorised agents.

3. What is the stipulated timeline for the competent authority to publish the list of all public services to be delivered through electronic mode?

A. 180 Days.

1.9 ACTIVITY

Elaborate the pros and cons of the Electronic Delivery of Services Bill, 2011 along with the critiques with respect to it. (800 words)

Unit 2: Rules and Regulations related to Cyber Cafe

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Legislative framework for Cyber Cafes in India

1.4 Guidelines pertaining to establishment of Cyber Cafes in India

1.5 Let's sum up

1.6 Further reading

1.7 Check your progress: Possible answers

1.8 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Cyber Crimes through Cyber Cafes
- Rules and Regulation governing Cyber Cafes
- Due Diligence pertaining to the establishment of Cyber Cafes

1.2 INTRODUCTION

Cyber Cafe is internet access point for public and it is been observed that public access point are the most obvious places used by cybercriminals, where visitor data can be usually hacked due to lack of awareness of Cyber-crime in Visitors as well as their identity is difficult to reveal as they are making use public internet point.[120] Many Cyber Cafes are now providing Wi-Fi services for their customers. Due to lack of awareness of cybersecurity many Cyber Cafe Visitors make mistakes such as making use of unencrypted devices or protocols, not logging out after work is

[120]Rangaswamy, Nimmi. (2009)The non/formal business of cyber cafés: A case/study from India. J Inf., Comm, Ethics in Society

completed, simple password, same password for multiple sites, Information left on the hard drive, not clearing browser history, storing of data on public hard disk, not checking for illegal or malicious software before using public machine which results in loss to the Visitors. In 2013 report by Symantec 56 percent access their social networking account using public Wi-Fi unsecured network, 29 percent access their bank account, 54 percent access personal mail, 29 percent do online shopping, 3 out of 10 do not log off after using public Wi-Fi network and 39 percent do not take any special steps to protect themselves when using public Wi-Fi. Cyber-crimes can take place when pubic internet access points such as Cyber Cafes are used if security mechanisms are not used. Types of Cyber-crimes that have taken place through Cyber Cafe are credit card fraud by making use of key logger software, online share trading fraud, Email account hacking, phishing, Cyber terrorism, Malicious code like worms, virus etc.[121] Section 43, 66, 67, 69 and 70 of the Information Technology Act read with the relevant provision of Indian Penal Code, cover myriad of cybercrimes, which can be committed through Cyber Cafes-

- Harassment via a fake public profile on social network site;
- Online Hate community;
- Credit Card Fraud;
- Introduction of viruses, Backdoors, Trojans and Bugs;
- Cyber Terrorism;
- Online Sale of illegal Article;
- Cyber Pornography;
- Phishing and Email Scams;
- Tax Evasion and Money Laundering;
- Theft of Confidential information;
- Online Share Trading Fraud.
- Cyber Stalking

Information Technology Act 2000 is a legal framework created and implemented to prevent Cyber-crime and amendments have also taken place for it but still improvements are required.

[121]Haseloff, M A [2005], *Cybercafés and their Potential as Community Development Tools in India*, The Journal ofCommunity Informatics, Vol 1 no 3 pp53-64

Today Indian cyberspace has an increase in spam and phishing activities, spread of botnets, virus, worms and malicious code are also on the rise. This has made India to be figured out as an active source in spreading malicious infection in computers, which is generally observed in developing countries.

Cyber Crime is not defined officially in the IT Act or in any other legislation. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislation. Hence, the concept of cybercrime is just a ***"combination of crime and computer".***

1.3 LEGISLATIVE FRAMEWORK FOR CYBER CAFES IN INDIA

An Internet cafe or Cyber Cafe is a place, which provides Internet access to the public, usually for a fee. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public.The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a ***"Place of Public Amusement"***as defined under ***section 2 (9) of the Bombay Police Act, 1951 (Act XXII of 1951).*** In 1998 India introduced new Internet policy and Sify was the first ISP. Internet cafes are the primary form of Internet access for people as a shared access model, which is more affordable than personal ownership of computer system and Internet connections. LAN gaming centre was also one of the Cyber Cafe model where various players play game online. These players can be connected to various other players in some different locations.[122] These Cyber Cafes provide multiplayer games, which are popular. Gaming Cyber Cafe has a large demand in various countries by youth and children's and thus have become a popular model for earning the profit. Cybercafes have been started with the intention to provide Internet services and other services to its users. It is a definite place, where you can access the Internet for your emails, talking to your relatives through chat, voice and video. Cyber Café has become one of the businesses nowadays where you are charged in exchange for the services. The aforesaid café has several computer stations connected to LAN. There are resorts, hotels, motels and ships, which provides Internet access to the guests. Cyber cafés also give training to the person who does not know the usage of the

[122]Mancebo, François. (2003) Cybercafe

Internet and other activities available there. Cyber Café is defined under the Information Technology Act 2000 and rules and regulations to govern the cafes are mentioned under Information Technology Rules 2011.

1.4 GUIDELINES PERTAINING TO ESTABLISHMENT OF CYBER CAFES IN INDIA

In order to regulate Cyber Cafes, several states of India government Ministry of communication and Information Technology have passed regulations some under Information Technology Act (ITA) 2000 and some under the State Police Act. Now, the Information Technology Amendment Act, 2008 has made many significant changes in the prevailing laws of cyberspace applicable in India, one of which is regarding Cyber Cafes. Information Technology (Amendment)Act, 2008 has provided a specific definition for the term ***"cyber café"*** and also included them under the term ***"Intermediaries"***. Several aspects of the Act, therefore become applicable to Cyber Cafes. The government of India has taken initiatives by the mean of Act to provide cyber security for Cyber Cafe.[123]These are the following steps need to be followed by Cyber Cafes under ***Information Technology (Guidelines for Cyber Cafe) Rules, 2011***-

1. ***Registration of Cyber Café***

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all cyber cafes shall be registered with a URN (Unique Registration Number) through an agency called as registration agency has been notified by the State Government in this regard. The requirements of registration shall include: Name of establishment, date of incorporation, Address with contact details including email address, Whether individual or partnership or sole proprietorship or society or company, Owner's name, Type of service to be provided from cyber café, Whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies).

2.*Identification Of User*

[123]'Cyber Cafes Under ITA 2008' (Naavi.org, 2020) <https://naavi.org/cl_editorial_09/edit_jan07_itaa_analysis_7_cyber_cafe.htm>

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all Cyber Cafes should not allow any person to access the services of cyber café without user identity. The user is supposed to produce certain documents before having access to the services of the cyber café so that proper identification of the user is known. Such documents are as follows: Identity card issued by any School or College, Voter Identity Card or Permanent Account Number issued by Income-Tax Authority or Photo Identity Card issued by the employer or any government agency or Passport or Driving License issued by the Appropriate Government or Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

3.*Log Register*

In accordance with Under Rule 5 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011, after the identification of the user and any person associated with him has been established as per sub-rule (1) of rule 4, the Cyber Cafe shall register and maintain the required information of each user as well as associated person in the log register for a minimum period of one year.The Cyber Cafe shall maintain an online version of the log register. This online version of log register shall be checked by using digital signature and should contain details including Name, Address, Gender, Contact Number, Date, Type and detail of identification document, Computer terminal identification, Log in Time and Log out Time.

A monthly report of log register including date-wise details and use of computer resource shall be prepared and there shall be the submission of hard copy and soft copy to the agency of registration or person as pointed out by the registration agency by the 5th of every month.History of websites accessed by the user using computer resource at cyber café. Logs of proxy server installed at a cyber cafe. Cyber Cafe may refer to "Guidelines for auditing and logging – CISG-2008-01" prepared and updated from time to time by Indian Computer Emergency Response Team. Cybercafe shall ensure that log register is not changed and it is been maintained in a secure manner for a period of at least one year.[124]

4.*Management and Administration Of Physical Layout And Computer Resource*

[124]Keniston, K and D. Kumar, (2004) Ed *Bridging the Digital Divide: Experience in India*,London,Sage Publications

In accordance with Under ***Rule 6 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011,*** Cyber Cafes shall adhere to following guidelines-

1. Partitions of Cubicles put inside the Cyber Cafe, should not surpass four and a half feet in the range from the floor level.
2. The screen of all PCs introduced other than in Partitions or Cubicles should be confronted 'outward', i.e. they should confront the regular open space of the Cyber Cafe.
3. Any Cyber Cafe having work areas or segments might not enable minors to utilize any PC asset in desk areas or allotments aside from when they are recognized by their gatekeepers or guardians.
4. All-time checks and servers introduced in the Cyber Café of the PC framework should be coordinated with the IST (Indian Standard Time).
5. All the PCs in the cyber cafe might be furnished with the monetarily accessible security or separating programming in order to maintain a strategic distance from quite far, access to the sites identifying with erotica including kid smut or disgusting data.
6. Cyber Cafe should take vital measures to guarantee that their PC asset is not used for any unlawful activity.
7. Cyber Cafe might show on the PC that review the explicit destinations on PC is prohibited and one ought to do nothing which is against the law or illicit.
8. Cyber Cafe should make essential measures to not permit the client from meddling with the PC framework settings.
9. Client personality data and log enlist ought to be kept up by cyber bistro in a secure way.
10. Record of the cyber bistro's staff might be kept up for 1 year legitimately.
11. Cybercafe might not abuse or change the data in the log register Information Technology Rules-2011

5.*Investigation of Cyber Cafe*

In accordance with Under Rule 7 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 an officer authorized by the registration agency, is authorized to check or inspect cyber cafe and the computer resource of the network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

A Cyber Cafe Owner is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central Government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly
defined with three-year imprisonment, which is also cognizable, bailable and compoundable.
There are many government stakeholder agencies formed for a secure computing environment and adequate trust and confidence in an electronic transaction.[125]

In India, many individuals go to Internet bistro to complete their everyday online exercises. Web cafes, or cybercafés, are spots that give administrations of web and different exercises and consequently clients need to pay them according to the time they have gotten to the administrations. Web cafes can be set up in genuine eating/drinking foundations, voyage ships, or different sorts of areas. Other than utilizing the PC workstation, you may likewise have the capacity to print or sweep reports, contingent upon the Internet cafe.[126] Yet, today the matter of Cyber Café has been declining in light of the fact that individuals get access to web at home, as they have the wideband association at home. Building up the cyber bistro is not a major ordeal, it has fewer prerequisites as contrast with different organizations however proprietors must be more secure on the grounds that cyber wrongdoing is been expanding in the present-day world.

1.5 LET'S SUM UP

[125]HaseloffAnikar M. - "Cybercafes and their Potential as Community Development Tools in India "- The journal of community informatics - Vol-1 No-3 2005 <http://ci-journal.net/index.php/ciej/article/view/226/181>
[126]GadgeReena K, Dr.MeshramB.B.,"Detect and Prevent Threats in Websites"-IJCST-International Journal of computer science and Techno- vol 3, Issue 1, Jan. - March 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

In this chapter, we have studied the meaning of cyber café along with a legislative framework for cyber cafes in India. Finally, we have ended our discussion with the guidelines that need to be followed by the cyber cafes as per the Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

1.6 FURTHER READING

- Singh, Umrav. (2016). Cyber Laws in India.
- Rangaswamy, Nimmi. (2009). The non/formal business of cyber cafés: A case/study from India. J. Inf., Comm, Ethics in Society. 7. 136-145. 10.1108/14779960910955855.
- Internet Privacy in India — The Centre for Internet and Society, Cis-india.org (2019), https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india (last visited Nov 20, 2019).
- Citeseerx.ist.psu.edu (2019),

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Cyber café?

Cyber Cafe isan internet access point for public and it is been observed that public access point are the most obvious places used by cybercriminals, where visitor data can be usually hacked due to lack of awareness of Cyber-crime in Visitors as well as their identity is difficult to reveal as they are making use public internet point.

2. Short note on legislative framework of cyber café in India?

An Internet cafe or Cyber Cafe is a place, which provides Internet access to the public, usually for a fee. It includes any commercial establishment or Internet kiosk, the objective of which is to make Internet services available to the general public.The fee for using a computer is usually charged as a time-based rate. Cyber Cafe is considered to be a ***"Place of Public Amusement" as defined under section 2 (9) of the Bombay Police Act, 1951*** (Act XXII of 1951). In 1998 India introduced new Internet policy and Sify was the first ISP. Internet cafes are the primary form of

Internet access for people as a shared access model, which is more affordable than personal ownership of computer system and Internet connections.

3. **How do you register a cyber café?**

Under Rule 3 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 all cyber cafes shall be registered with a URN (Unique Registration Number) through an agency called as registration agency has been notified by the state Government in this regard. The requirements of registration shall include: Name of establishment, date of incorporation, Address with contact details including email address, Whether individual or partnership or sole proprietorship or society or company, Owner's name, Type of service to be provided from cyber café, Whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies).

4. **Short note on investigation of cyber café?**

In accordance with Under Rule 7 of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 an officer authorized by the registration agency, is authorized to check or inspect cyber cafe and the computer resource of network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

A Cyber Cafe Owner is expected to preserve and retain such information as may be specified for particular duration and in such manner and format as the Central government may prescribe and on failure to do so he may be punished with an imprisonment for a term, which may extend to three years and shall also be liable to fine. Thus, the responsibility of Cyber Cafes has now been clearly

defined with a three-year imprisonment, which is also cognizable, bail able and compoundable.

1.8 ACTIVITY

Explain the guidelines pertaining to establishment of cyber café in India along with a case study. (1000 words)

Unit 3: Rules and Regulations related to Service Provider's Liability

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Internet Service Provider (ISP)

1.4 Liability of Network Service Providers

1.5 Internet Service Providers Liability in India

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible Answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of Internet Service Provider
- Intermediaries Liability
- Liability of Service Provider and Section 79 of Information Technology Act
- Copyright Act and Intermediaries

1.2 INTRODUCTION

Origin of internet has raised many atypical issues that do not find an express solution in the existing legal dominion. The atypical power of scattering engendered by the web, a power that ordinary users can utilize, has created a new and grinding challenge to the ability of copyright

holders to enforce their ownership of intellectual property. The chief threat to copyright holders by the internet's untangle information distribution is online piracy. The scope of this problem is hard to define in concrete terms. Though the damage of online piracy is hard to evaluate in monetary terms, a driving motivation to protect the copyright holder remains. The widespread and open copyright abuse is feared and will a systematic cultural disregard for the author's intellectual property rights.

1.3 INTERNET SERVICE PROVIDER (ISP)

One of the salient features and equivocal issue associated with the fast-developing online industry is the liability of services providers are gateway to the world of cyberspace. They provide online access to individuals, educational, institutions, and government agencies. Those entities include online service providers, those who provide content through networks in addition to internet access, which is provided through the same networks and internet service providers who provide direct access to the internet and usually have content provided in direct location. The service providers are commercial and non- commercial entities that connect users to the internet, provided the user has access to the necessary hardware for this interface, namely telephone line and, modern and a personal computer.[127]

The liability of the service provider for copyright infringement can be fixed only when his position, powers and limitations are clearly understood. The Internet began as a closed network between government research laboratories and universities and colleges. As universities and colleges began giving Internet access to their faculty and other employees, ISPs were created to provide Internet access to those employees at home and elsewhere. The first ISP began in 1990 as The World, based in Brookline, Massachusetts.

Individual customers and businesses pay ISPs for Internet Access. ISPs are interconnected to one another at network access points. In turn, ISPs pay other, larger ISPs for their Internet access, which in turn pay still other ISPs. This cascades multiple times until transmissions reach a Tier 1 carrier, which is an ISP capable of reaching every other network on the Internet without

[127] B. Rowe, D Wood, D Reeves, and F Braun, "The Role of Internet Service Providers in Cyber Security", Institute for Homeland Security Solutions, Applied research* Focus result, 2011 <http://sites.duke.edu/ihss/files/2011/12/ISPProvided_Security-Research-Brief_Rowe.pdf>

purchasing IP transit or paying settlements. However, it is difficult to determine the status of a network because the business agreements to pay settlements are not made public.

1.4 LIABILITY OF NETWORK SERVICE PROVIDERS

According to section 79, of the IT Act[128]For the removal of doubts, it is hereby declared that "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention."

Explanation.—for the purposes of this section,—

(a) ***"network service provider"*** means an intermediary; (b) ***"third party information"*** means any information dealt with by a network service provider in his capacity as an intermediary;

(b) This section seeks to restrict the liabilities of a network service provider in certain cases. Meaning of the term "network service provider" (NSP): Section 79 says that an NSP is an intermediary.

The IT Act has defined the term "intermediary" -

According to ***Section 2(1)(w) of the IT Act "intermediary"*** with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

1. It receives the message on behalf of another person, or

2. It stores the message on behalf of another person, or

3. It transmits the message on behalf of another person, or

4. It provides any service with respect to that message

[128](Cc.iitd.ernet.in, 2020)
<http://www.cc.iitd.ernet.in/misc/liability-network-service-providers.pdf> accessed 24 April 2020.

The term ***"electronic message"*** has not been defined in the IT Act. The UNCITRAL Model Law on E-commerce defines a data message as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy".[129]

Note: The IT Act has been based largely on the UNCITRAL Model Law on Ecommerce.

The IT Act has inserted ***section 88A into the Indian Evidence Act.*** This section relates to an electronic message forwarded through an electronic mail server. After considering the definition of data message under the UNCITRAL Model Law and the context of electronic message under section 88A of the Indian Evidence Act, it may be concluded that the term NSP is a narrow term that relates to electronic message service providers only (such as email service providers). It does not apply to other service providers such as search engines, auction websites etc. Even for Internet Service Providers (ISP), the benefits of this section would extend only to the email, voicemail, telephony etc services provided by them and not to the Internet connection services offered by them. However, this section must be read in conjunction with ***section 85 of the IT Act*** that relates to liabilities of companies. This is discussed in the next chapter of this book.

The restrictions on the liabilities of NSPs. An NSP is not liable for any third party information or data made available by him if:

1. The NSP proves that the offence or contravention was committed without his knowledge, or
2. The NSP proves that he had exercised all due diligence to prevent the commission of such offence or contravention.

The important terms used in this section are: Knowledge implies "clear perception of a fact" or ***"specific information".*** Liability of ISPs in India In respect to ISPs in India, their liabilities are also determined by the License for Internet Services based on guidelines dated 24th August, 2007. The license as applicable on 30th October 2007 is provided in the CD ROM accompanying the ASCL publication titled ***"Fundamentals of Cyber Law".***

<u>According to clause 33 of this license:</u>

[129] H E Pearson, "Liability of Internet Service Providers", 1996 <http://www.leginetcy.com/articles/Liability%2 0of%20Internet%20Service%20Providers.pdf>

1. ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content.[130]

2. Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

3. ISPs must ensure that content carried by them does not infringe "international and domestic cyber laws".

4. The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.

5. ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.

6. ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.

7. ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.

8. ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.

9. ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

1.5 INTERNET SERVICE PROVIDERS LIABILITY IN INDIA

In India, the law applicable to the infringer swing upon which part of law deals with that certain infringement. Therefore, due to the lack of such law, the Copyright Act and the Information Technology Act includes the liability of ISP's:[131]

[130]What is an Internet Service Provider (ISP)? - Definition <https://www.techopedia.com/definition/2510/internet-service-provider-isp>

- ***Copyright act 1957***

As per ***Section 51(a) (ii) of the Copyright Act***;

"the Indian Copyright Act, the act of infringement is when, a person without any license by the registrar or the owner of the particular copyright, does an act that is in the contravention of the conditions of a that license or condition imposed by a competent authority under this Act permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he is unaware as and had no reason to believe that the particular communication to the general public would result in copyright infringement."

Nowadays the Internet service providers, instruct their servers transmit and store their users' data across the network. This act of ISP's helps them to hold any third party liable in case of any infringement. In order to be liable for the infringement, it is very necessary that the ISP should benefit financially from it. The ISP's earn even if they offer some copyrighted illegal material because of the advertisements that come along with it. Therefore, an ISP can be held liable not only when they transmit such infringed material but they are liable even if they store it.

- ***Criminal Liability***

An ISP can be held criminally liable when he does an act of infringement or abets infringement of:

(a) the copyright in a work, or

(b) any other right conferred by this Act, If a person does such an act than the Copyrights Act provides for the punishment to be given to him, i.e of imprisonment which may extend to one year, or with fine, or with both.[1]

However, the Copyright Act clearly states that the ISP can be held liable only in the case he was unaware infringing material stored or being transmitted through their servers. This provides an exception to the liability.

- Information Technology Act, 2000

---

[131] Liability of Network Service Providers
<http://www.cc.iitd.ernet.in/misc/liability-network-service-providers.pdf>

Section 79 of the Information Technology Act states the ISP (a Network service provider in the case of this act) as an "Intermediary", which is defined as " any person who on behalf of any other person receives, transmits or stores any message or provides any service with respect to any message."[2] This section also provides that, no ISP can be held liable if he proves that he was unaware of the infringement that was caused by the third party that he had exercised all due diligence to prevent the commission of such offence.[132]

Therefore, the ISP can get away from being liable for the copyright infringement if it is proved under this section[3]

(a) That the ISP was unaware of the infringement,

(b) That he took all the due diligence to prevent such infringement.

However, data has passed through an ISP's servers or stored in them, that is likely to infringe the copyright of another, it is considered that such ISP had to have 'knowledge' of such data and he has the duty to take appropriate measures to prevent such infringement. In such a case, the ISP cannot take a defence that he was unaware of such infringement.

A person is said to have done an act with due diligence when in the layman's terms he had done that act or prevented an act by reasonable standards expected out of a prudent person who is said to have the knowledge about such illegal activity.[4]

- Drawbacks of Copyright Act

(a) The IT Act provides wider scope to the authorities to harass ISPs in matters where their liability is the question.

(b) Which actions can be termed as done with 'due diligence' is not defined anywhere in the act.

(c) Who is an ISP? The answer to this question is not given under the IT Act. Also, the IT Act does not provide for the liability of the ISP. The liability of ISP is as same as for anyone who is simply a communication carrier.

[132] Network Service Providers Not to be Liable <https://meity.gov.in/content/network-service-providers-not-be-liable-certain-cases>

There is an urgent need to incorporate certain laws or bring amendments in the acts because the absence of specific laws regarding the liability of the ISP in the Indian Law results in the ISP's escaping the liability in case of infringement. In order to make way for resonate legislation with regard to ISP liability in India, it is essential to label some of the key subjects mentioned hereunder;

a) There is an acute need to provide a definition of Internet Service Provider. Unless it is done, it would always create confusion as to who can be put under the liability. It is also important to define "due diligence"

b) Effective tools like DCMA can be used. Various effective measures should be adopted so that the liabilities of ISP's are clearly identified.[133]

c) It should be made sure that, the Information Technology Act makes it obligatory for ISPs to terminate services of subscribers who frequently violate.

1.6 LET'S SUM UP

In this chapter, we have studied the concept of Internet Service Provider along with the liability of network service provider and provisions pertaining to it. Finally, we have ended our discussion with Internet Service Provider's liability in India and the relation between intermediaries and Copyright Act.

1.7 FURTHER READING

- Suresh.T.Vishwanathan.,*"The Indian Cyber Law"*, 1st Edition, 2000, Bharat Law House, New Delhi, p.96.
- Prof.S.R. Bhansali., *"Information Technology Act, 2000"*, 1st Edition, 2003, University Book House Pvt. Ltd, Jaipur, p. 218.
- NandanKamath., *"Law Relating to Computers, Internet and E-Commerce"*, 2nd Edition, 2000, Universal Law Publishing Co.Pvt.Ltd, Delhi, p. 2.

[133]Copyright Infringement And The Liability Of Internet <https://blog.ipleaders.in/copyright-infringement-liability-internet-service-providers/>

- Rahul Matthan., *"The Law Relating to Computers and the Internet"*, 2000, Butterworths India, Delhi, pp. 428-429.
- Raman Mittal., *"Online Copyright Infringement Liability of Internet Service Providers"*, 46 JILI (2004), p. 289.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Internet Service Provider?

They provide online access to individuals, educational, institutions, and government agencies. The service providers are commercial and non- commercial entities that connect users to the internet, provided the user has access to the necessary hardware for this interface, namely telephone line and, modern and a personal computer.

2. Define 'Intermediary' under IT Act?

According to section 2(1)(w) of the IT Act "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

3. What are the characteristics of NSP?

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

- It receives the message on behalf of another person, or
- It stores the message on behalf of another person, or
- It transmits the message on behalf of another person, or
- It provides any service with respect to that message.

4. What is the liability of the ISP under Copyright act?

As per Section 51(a) (ii) of the Copyright Act, "the Indian Copyright Act, the act of infringement is when, a person without any licence by the registrar or the owner of the particular copyright, does an act that is in the contravention of the conditions of a that licence or condition imposed by a competent authority under this Act permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement

of the copyright in the work, unless he is unaware as and had no reason to believe that the particular communication to the general public would result in copyright infringement."

1.9 ACTIVITY

Explain the liability of Internet service providers in India with an illustration or case study. (800-1000 words)

Unit 4: E-Health and Regulatory Framework

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Concept, functionalities and benefits

1.4 Electronic Health Records

1.5 Basic functions and elements of EHR

1.6 Investment in E-Health

1.7 Legal and Regulatory Framework

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept, functionalities and benefits of E-Health
- Electronic Health Records
- Enactments of different laws pertaining to E-Health

1.2 INTRODUCTION

As per the World Health Organization ("WHO"), E-Health means "the use of information and communication technologies ("ICT") for health". The definition, though very concise, is not very helpful. The European Commission has put forth a more elaborate definition of e-Health. e-Healthrefers to "tools and services using information and communication technologies that can

improve prevention, diagnosis, treatment, monitoring and management". Therefore, the expression e-Health may be safely said to include both tools and services that use ICTs for purposes connected to health.[134]

For several years now healthcare services have been facing pressure by citizens, patients, professionals and also by public and private institutions. The ageing of the population, higher standards of living, and more informed and educated citizens mean that both patients needs and patient expectations are growing. These rising demands, along with the appearance of new and costly health technologies and increasing budget restrictions, invite health managers to invest wisely in ICT and to carefully assess its opportunity cost in the current context of rising health expenditure and economic crisis.[135]

Investment in eHealth should be considered a decision of key importance for the health system. This means there must be, in addition to an accurate estimate of costs, an evaluation of its benefits, both in economic terms and in terms of improved quality and efficiency in the services provided. Nowadays, ICT tools must be included among the many instruments used in a health system, whose functioning can hardly be conceived without tools of this type.

1.3 CONCEPT, FUNCTIONALITIES AND BENEFITS

The concept of eHealth encompasses applications as diverse as electronic health records, different types of telemedicine, epidemiological surveillance, health portals, management systems and distance learning programs focused on health and medicine. Its users and beneficiaries are equally diverse. The applications help meet the needs of health professionals, those of patients and their families, those of healthcare authorities and experts and also those of input and service providers, among others.

There can be no doubt that eHealth represents an equitable, effective and efficient way to increase accessibility, safety and quality in healthcare. eHealth tools can be used to increase the availability of medical resources, thus optimizing care processes. They enable specialized

[134] Michael Kirby, Medical Technology and New Frontiers of Family Law, 1 AUSTL J FAM L 196, 212 [1987]
[135] Oh, Hans &Rizo, Carlos &Enkin, Murray &Jadad, Alejandro. (2005). What is eHealth? A systematic review of published definitions. World hospitals and health services: the official journal of the International Hospital Federation. 41. 32-40

knowledge to be taken to different places or to isolated locations, through distance appointments or teleconsultation. They facilitate the provision of timely healthcare, partnership projects, etc. They can also help reduce the costs incurred by systems and by families.[136]

In eHealth, two large spheres can be distinguished from one another, for purposes of analysis. There is, on the one hand, what is known as health informatics, that is, technological solutions for applications used to provide care, which allow information to be recorded and processed: electronic health records and department-specific applications, population management systems and systems that support planning and management are a few examples. And, on the other hand, there is telemedicine, which refers to health services and care provided from a distance. Applications already exist for many of the specialities: tele radiology, tele cardiology, tele dermatology, tele ophthalmology, tele pathology, tele psychiatry, and others.[137]

The case of tele radiology is a clear example of the advantages of telemedicine. Small or rural communities that cannot sustain an on-staff radiologist can benefit a great deal from the professional activity performed at a distance. Local hospitals can send images to a larger care center in order to obtain a second opinion, whether from the general radiologists who work in such centers or from radiologists with particular subspecialties. Emergency rooms can send, any time day or night, their images to affiliated centers or even to the homes of radiologists. Tele radiology as a teaching tool, can also enhance the quality of ongoing medical training. And finally, tele radiology offers direct benefits to the patient, by reducing the costs of transportation, accommodations and board that would be incurred if the patient had to travel to where the doctor is based.

The use of ICT can also bring significant improvements to the management of public health, in terms of areas of surveillance and also in the planning and overseeing health service management. ICT tools contribute to the design of safer, timelier and more reliable processes for data gathering and storage and also to better statistical use of the information. This has positive repercussions on the effectiveness and efficiency of the macro system that encompasses

[136] Ashok VikhePatil, K V Somasundaram and R C Goyal; Current Health Scenario In Rural India <http:// www.sas.upenn.edu/~dludden/WaterborneDisease3.pdf>

[137] Awski, Szymon&Saberwal, Gayatri. (2014). IneHealth in India today, the nature of work, the challenges and the finances: An interview-based study. BMC medical informatics and decision making. 14. 1. 10.1186/1472-6947-14-1

everything from the analysis of health needs and problems to the evaluation of health outcomes obtained in the population.[138]

1.4 ELECTRONIC HEALTH RECORDS

An Electronic Health Record (EHR) is a digital version of a patient's health records. EHRs help eliminate the problems associated with physical records such as loss and lack of accessibility. EHRs can be stored centrally and accessed at any time, irrespective of where or when the information was collected. With EHRs, doctors are able to view their patient's complete medical history even if they are treating the patient for the first time. This would help reduce duplication of tests and facilitate the secure exchange of information, which in turn helps the patient and the healthcare facilities manage costs.

1.5 BASIC FUNCTIONS AND ELEMENTS OF EHR

While EHRs were initially developed to document clinical care, most can perform additional functions that can support good quality care. Common functions of EHRs include (Health Resources and Services Administration, 2014a).

- Recording patient demographics and care management data on patient visits.
- The clinical decision supports.
- Reports required for financial management, quality assurance, chronic disease management, and public health data collection.
- Consents, authorisations, and directives.
- Interfaces and interoperability required to exchange health information with other clinicians, laboratories, pharmacies, patients, and government disease registries.
- e-prescribing.
- Alerts and reminders.
- Medication reconciliation.

[138] Marcus E, Fabius R. What is E-health?
<http://www.acpenet.org/ Forums/Topical/Ehealth/Primer.htm>

- Commonly used screening tools and checklists.
- commonly used forms for schools, camps, and sports participation.
- Patient education.

Some systems might also include integrated practice management support that enables functions like billing, online scheduling, and patient portals. Examples of some basic elements of EHRs are provided below. This list is not exhaustive and designed to provide a glimpse into EHRs and some of their capabilities.

Some of the benefits of EHR can be classified into the following types:

- ***Accessibility and Availability***

Paper charts are for single users; they can only be seen by one person in one place. EHRs can be used by more than one person at a time, and they can also be accessed from different locations. This is one of the benefits that new users most quickly come to appreciate.[139]

- ***Multiple display modes***

EHRs also have the potential of offering various ways to view the information, since users sometimes prefer to see information in different formats depending on their needs. A good EHR must allow data display to be configured in different ways, offering these options to users. Another useful function in clinical practice is to be able to view trends. These can be generated instantly, by putting the trends shown by a lab value or a vital sign (such as blood pressure) into graphic form.

- ***Communication with other professionals***

EHR systems can serve as vehicles for communication among professionals. This capability need not be limited to physician-to-physician communication, but can also include other members of the healthcare team. Many EHR systems include features similar to e-mail or instant messaging, thus allowing the different professionals to send messages to other professionals involved in the care of this patient.

- ***Communication with patients***

[139] Bhatia JC, Cleland J: Health-care seeking and expenditure by young Indian mothers in the public and private sectors. Health Policy Plan 2001, 16(1):55–61

EHRs can also improve communication with patients. As mentioned above, the personal health record can potentially be used as a communication channel between the patient and the health team caring for the patient.[140]

- ***Data aggregation***

EHR systems also have data collection capabilities, which makes it possible to create data groups and summaries. To ensure effective data aggregation, it is vital that data quality be very carefully controlled and that medical knowledge is correctly represented (through the use of semantic constraints). This functionality can be applied to the reuse of stored information for purposes of clinical management, clinical research or the preparation of public health reports.

- ***Access to knowledge bases***

Another potential benefit of using an EHR system is that it permits access to knowledge bases in a contextual manner. This means that the EHR can provide contextual information concerning each patient and provide the user with information that is useful in decision-making, extracted from different knowledge bases.

- ***Integration with decision-making support systems***

Decision-making support is the ***raison d'être*** of EHRs. The aim of these applications is to contribute to the care process, offering support to professionals, showing updated contextual information and suggesting alternatives to their decisions. These computerized decision-making support systems are difficult to achieve and are not very advanced due to the complexity inherent in their development and implementation. They consist of a rule engine that uses information based on the patient (from his or her EHR) and information based on scientific knowledge (from the system's knowledge bases), with which they generate different outputs, such as reminders, alerts, diagnostic or treatment suggestions based on the automation of clinical practice guides, etc. Their ultimate goal is to prevent errors and to enhance care quality.[141]

- ***Cost benefits***

The issue of whether EHR system implementation brings cost benefits is a controversial one, with literature containing evidence in both directions. This inconsistency arises in part because of

[140]Loman P. E-Health: 'Putting health on the Net'. An FCG White Paper <http://www.fcg.com/webfiles/whitepaper/white_paper_files/wpEhealth.asp>

[141] Reddy KS, Patel V, Jha P, Paul VK, Shiva Kumar AK, Dandona L: Towards achievement of universal health care in India by 2020: a call to action. Lancet 2011, 377(9767):760–768

the different perspectives used for analyzing returns on investment (ROI) (the individual physicians, service providers, insurance companies, governments) and the type of health care system that predominates in each country. More information is needed before more precise calculations can be made of the ROI related to EHR systems.

1.6 INVESTMENT IN E-HEALTH

The healthcare sector as an industry is expanding rapidly in India and has not been as severely impacted by the economic slowdown as some of the other industries.India, one of the biggest emerging markets, is currently an important destination for Foreign Direct Investment ("FDI").[142]A significantly low presence of doctors in rural and semi-urban areas has led to limited access to proper healthcare facilities for people living in these areas. Telemedicine and e-Health are considered to be some solutions to this lack of access. The growth of the IT sector in India (which plays a crucial role in telemedicine) has led to the emergence of this sector in India. Tele-radiology has emerged as a fast-growing area with an increasing number of foreign hospitals active in this space. These hospitals consult Indian experts to provide opinions, i.e., on x-rays of patients in the hospital. Many hospitals have adopted the public-private partnership route to render services through telemedicine.

Some investment options are:

a) FOREIGN DIRECT INVESTMENT

Foreign investment into India is governed by the Foreign Exchange Management Act, 1999 ("FEMA"), the rules and regulations made by the Reserve Bank of India ("RBI"), and the Industrial Policy and Procedures issued by the Ministry of Commerce and Industry through the Secretariat for Industrial Assistance, Department of Industrial Policy and Promotion ("DIPP").[143]

The provisions pertaining to FDI are laid down in Schedule I of FEMA (Transfer or Issue of Security by a Person Resident outside India) Regulations, 2000.While the DIPP issues policy

[142] Oracle Corporation. CEO Perspective: Health Care Information Technology <http://www.hciv.com/profiles/oracle.pdf>

[143] Consolidated FDI Policy, Government of India, Ministry of Commerce & Industry, Department of Industrial Policy & Promotion, SIA (FC Division) <http://dipp.nic.in/ English/policies/FDI_Circular_2016.pdf>

guidelines and press notes/releases from time to time regarding foreign investment into India, it also issues a consolidatedpolicy on an annual basis ("Consolidated FDI Policy"). Currently, foreign investment is regulated by the Consolidated FDI Policy of 2016.100% FDI is permitted in most sectors under the automatic route, i.e., where prior approval of the government, specifically the Foreign Investment Promotion Board ("FIPB"), is not required. Generally, there are no restrictions prescribed for e-Health services, and therefore FDI up to 100% should be permitted without government approval. It may also be noted that FDI is permitted up to 100% under the automatic route in the hospital sector and the manufacture of medical devices. In the pharmaceutical sector, FDI is permitted upto 100% in Greenfield projects and 74% in Brownfield projects under the automatic route and FDI beyond 74% in Brownfield projects requires FIPB approval. Greenfield projects are new projects that are coming up in India while Brownfield projects are existing projects in India.

b) FOREIGN VENTURE CAPITAL INVESTMENT

Another vital means of investment is through venture capital investment by entities registered with the Securities Exchange Board of India ("SEBI") as foreign venture capital investors. While it is not mandatory for a private equity investor to register as a Foreign Venture Capital Investor ("FVCI") under the FVCI regulations,[144] there are some significant advantages to be gained by registering as an FVCI. An FVCI is exempt from compliance with the pricing guidelines under the Consolidated FDI Policy for the acquisition of securities at the time of entry as well as for the transfer/sale of securities at the time of exit. Secondly, in cases where thepromoters of the company intend to buy back the securities from an FVCI, they are exempted from making an open offer under the Takeover Code. It should be noted that SEBI has been granting approvals to FVCIs only for investments in certain identified sectors, amongst them being researchand development of new chemical entities in the pharmaceutical sector, and units of SEBI registered Venture Capital Funds ("VCFs"). Further, the Reserve Bank of India ("RBI") has made recent amendments to the foreign exchange control regulations to permit FVCIs to invest in SEBI registered Alternate Investment Funds ("AIFs").[145]

[144] SEBI (Foreign Venture Capital Investor) Regulations, 2000

[145] SEBI introduced SEBI (Alternate Investment Funds) Regulations, 2012 to govern domestic pooling vehicles. RBI has issued Notification no. FEMA. 355/2015 that permits AIFs and other investment vehicles to accept foreign investments under the automatic route

1.7 LEGAL AND REGULATORY FRAMEWORK

a) THE I.T. ACT, 2000

E-Health involves a constant exchange of information between the patient and the service provider. The patient's personal information, such as medical history and physiological conditions, are considered Sensitive Personal Data or Information ("SPDI") under the Data Protection Rules.[146] When a body corporate collects, stores, transfers or processes such information, certain requirements under the Data Protection Rules are triggered.Consent is one of the major requirements under the Data Protection Rules. Before a doctor or an institution does anything with a patient's data, they are required by law to obtain the recipient's consent in writing. The patient must be informed about the fact that the data is being collected, what it will be used for and whether it would be transferred to any third parties, along with the contact details of the agency collecting the information.

The Data Protection Rules also mandate the implementation of reasonable security practices and procedures in order to keep the SPDI secure. This requirement is fulfilled if the body corporate conforms to the international standard IS/ISO/IEC 27001 on "Information Technology-Security Techniques-Information Security Management System-Requirements" or similar standards that are approved and notified by the Central Government. As on date, no such standards have been notified.

In 2013, the Ministry of Communications and Information Technology came out with a clarification[147]which stated that body corporates that were collecting, storing, processing or transferring information out of a contractual obligation were not required to observe some of the requirements of the Data Protection Rules such as obtaining consent from the owner of the SPDI for collecting or disclosing the SPDI. The other requirements, however, must still be observed.

[146] Rule 3 of the Data Protection Rules defines Sensitive personal data or information of a person to mean such personal information which consists of information relating to (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information

[147] Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000 issued on 18th March, 2013
<http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules_1.pdf>

b) OTHER SERVICE PROVIDERS REGULATIONS UNDER THE NEW TELECOM POLICY, 1999 (OSP REGULATIONS)

Service providers who render "Application Services" - which includes telemedicine services – using telecom resources provided by telecom service providers, are required to be registered as an 'Other Service Provider' ("OSP") with the Department of Telecommunications.

c) THE DRUGS AND COSMETIC ACT, 1940

The D&C Act and D&C Rules regulate the manufacture, sale, import and distribution of drugs in India. In many foreign jurisdictions, there is a clear distinction between a drug that must be sold under the supervision of a registered pharmacist on the production of a valid prescription (signed by a registered medical practitioner) and those that can be sold by general retailers over-the-counter ("OTC"). OTC drugs have a different meaning in the context of Indian laws. The D&C Act requires that all drugs must be sold under a license.

The D&C Rules also state that prescription drugs can only be dispensed on the production of a prescription which is in accordance with the provisions of the rules. For a prescription to be considered valid under the D&C Rules, it must be in writing, signed and dated by the doctor issuing the prescription.

d) THE INDIAN MEDICAL COUNCIL ACT, 1956

The MCI Act provides that only those persons who have a recognized degree in medicine and are registered with one of state medical councils have the right to practice medicine in India. The MCI Code lays down professional and ethical standards of interaction of doctors with patients. The MCI Code also specifies that efforts are to be made to computerize medical records so that they can be retrieved quickly. Doctors are bound by the MCI Code and are required to submit a declaration to that effect. The apex body currently regulating the practice of medicine is the Medical Council of India. However, the proposed National Medical Commission Bill, 2016,[148] which has been drafted by the National Institution for Transforming India ("NITI Aayog"), intends to replace the current Medical Council of India with a 'National Medical Commission'. The passing of the National Medical Commission Bill would see a change in the current regulatory framework regulating medical practitioners.

[148] Proposed National Medical Commission Bill, 2016
<http://niti.gov.in/writereaddata/files/document_publication/MCI%20Bill%20Final.pdf>

e) THE CLINICAL ESTABLISHMENTS ACT, 2010

Establishments falling under the definition of a 'clinical establishment' under the Clinical Establishments Act would be required to register with the relevant authority and conform to the minimum standards as prescribed under the act. The Clinical Establishments Act is applicable in Arunachal Pradesh, Uttar Pradesh, Uttarakhand, Rajasthan, Bihar, Jharkhand, Himachal Pradesh, Mizoram, Sikkim and all Union Territories except the NCT of Delhi. Certain states such as Maharashtra and Karnataka have their own state clinical establishment legislations.

1.8 LET'S SUM UP

The e-Health market presents a lot of opportunities, but with every opportunity, there are bound to be risks involved. Innovation in this sector is yet to reach a saturation point, with new products frequently being introduced in the market. The legislative framework to protect and regulate such developments will remain one step behind, as it is yet to be seen how the industry will mature. Regardless, regulators have taken note of the restrictions, and in many cases, the absence, of the law and are striving to formulate forward-looking policies and legislations. The NIPR is only one such example.

The Ministry of Health and Family Welfare recently set up ten panels led by the top brass of the DCGI'soffice. They have been entrusted with the revision of the drug regulations in order to bring about ease in compliance and adopting to the progressive changes in the industry.

1.9 FURTHER READING

- Gambarte, M. L., Lopez Osornio, A., Martinez, M., Reynoso, G., Luna, D., et al. (2007). A practical approach to advanced terminology services in health information systems. Stud Health Technol Inform, 129, 621-625.
- Greenes, R. A. (2007). Clinical decision support - the road ahead. Amsterdam: Elsevier Academic Press.

- Heimly, V., Grimsmo, A., Henningsen, T. P., &Faxvaag, A. (2010). Diffusion and use of Electronic Health Record systems in Norway. Stud Health Technol Inform, 160 (Pt 1), 381-385.
- McDonald, C. J. (1997). The barriers to electronic medical record systems and how to overcome them. J Am Med Inform Assoc, 4 (3), 213-221.
- Simon, S. R., Kaushal, R., Cleary, P. D., Jenter, C. A., Volk, L. A., et al. (2007). Physicians and electronic health records: a statewide survey. Arch Intern Med, 167 (5), 507-512.
- Sujansky, W. V. (1998). The benefits and challenges of an electronic medical record: much more than a "word-processed" patient chart. West J Med, 169 (3), 176-183.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is E-Health?

As per the World Health Organization ("WHO"), E-Health means "the use of information and communication technologies ("ICT") for health".

2) What is EHR?

An Electronic Health Record (EHR) is a digital version of a patient's health records.

3) What are the functions of EHR?

Common functions of EHRs include (Health Resources and Services Administration, 2014a).

- Recording patient demographic and care management data on patient visits.
- The clinical decision supports.
- Reports required for financial management, quality assurance, chronic disease management, and public health data collection.
- Consents, authorisations, and directives.
- Interfaces and interoperability required to exchange health information with other clinicians, laboratories, pharmacies, patients, and government disease registries.
- e-prescribing.
- Alerts and reminders.
- medication reconciliation.

- Commonly used screening tools and checklists.
- commonly used forms for schools, camps, and sports participation.
- Patient education.

4) How does the I.T. Act aid in E-Health?

The patient's personal information, such as medical history and physiological conditions, are considered Sensitive Personal Data or Information14 ("SPDI") under the Data Protection Rules. When a corporate body collects, stores, transfers or processes such information, certain requirements under the Data Protection Rules are triggered.

1.11 ACTIVITY

Explain the meaning, concept, functions and elements of E-Health and Electronic Health Records along with the legal enactments with respect it? (1000 words)

Block 4
Laws related to Data Protection in India

Unit 1: Law related to Sensitive Personal Data in India

1

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Legal definition of ‘Personal Information’ and ‘Sensitive Personal Data or Information’
1.4 Procedure to collect the Sensitive Personal Information
1.5 Disclosure of the Sensitive Personal Information or Data
1.6 Transfer of Information
1.7 Failure to comply with the provisions
1.8 Points to be pondered upon
1.9 Recent legal updates
1.10 Let’s sum up
1.11 Further reading
1.12 Check your progress: Possible answers
1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is Sensitive Personal Data or Information
- Procedure to collect the Sensitive Personal Information
- To whom can disclosure of information be made

1.2 INTRODUCTION

The Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) isn’t exhaustive and did not specifically deal with the protection of electronic data, until the

Information Technology (Amendment) Act 2008 was passed and the IT Act, 2000 was amended accordingly to include certain provisions relating to electronic data. Further, to give effect to the then brought provision by the 2008 Amendment Act, the Central Government framed certain rules. Hence in the year 2011, the Central Government in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the IT Act, 2000, passed the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information to deal with personal information and also defined sensitive personal information, with which we are concerned here.[149] These rules are called "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (hereinafter referred to as the 2011 Rules).

1.3 LEGAL DEFINITION OF 'PERSONAL INFORMATION' AND 'SENSITIVE PERSONAL DATA OR INFORMATION'

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined as, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. It is however different from Sensitive Personal Data or Information. Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;

[149] Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233

vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

However, by virtue of the proviso to this rule, it excludes from its purview any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force.[150] And thus, this information which is so excluded by virtue of the proviso to Rule 3 isn't considered to be sensitive personal information for the purposes of the 2011 Rules.

1.4 PROCEDURE TO COLLECT THE SENSITIVE PERSONAL INFORMATION

The prerequisites of collecting or obtaining such data or information which has been covered under the definition of the Sensitive Personal Information as per ***Rule 3 of 2011*** Rules have been given under Rule 5 of the same. It includes:

(1) Consent

No Sensitive Personal Data or Information is permitted to be collected without the consent of the person whose information is being sought to be collected. Further, to ensure that this aspect of consent is well adhered to, the 2011 Rules provide that such consent by the provider must be in writing through letter or Fax or can be sent by email and the point worth noting is that the consent here is regarding the purpose of usage of such information. This consent is required before the collection of such Sensitive Personal Information or Data.

(2) Collection of Data must be necessary and for a lawful purpose

The 2011 Rules do permit the individual or entity to collect any information which would be covered under Rule 3 as Sensitive Personal Information or Data only when these 2 conditions are met:

(a) that the information which is sought to be collected is for a lawful purpose which is connected with any of his or its function or activity which in turn is also lawful; and

[150]Samuel Warren & Louis D Brandeis, "The Right to Privacy" Harvard Law Review 193 (1980)

(b) that collecting such sensitive personal data or information is necessary for that lawful purpose.

(3) Knowledge of the person giving the concerned information

The person or entity who is collecting information has to make sure:

(a)that the person whose information is being collected knows that such information is being collected;

(b) that the person whose information is being sought is aware of the purpose for which the concerned information has been collected;

(c) that such person is aware of the person/authority/institution who are likely to be the recipients of the information which is being sought from him;

(d) that such person knows certain details of the agency which is collecting such information as well as the one who will retain such information. Such information shall comprise of the names and addresses of the above-mentioned agencies.

And the person or entity seeking such sensitive personal information must take such reasonable steps as it deems fit and necessary to fulfil the conditions mentioned above.

(4) Also, the person or entity who is collecting the sensitive personal information is under an obligation to provide the person, from whose such information is sought, an option to not provide (or in other words, decline) whatever data or information which was sought to be collected. Discharge of this obligation has to be done by the concerned person or entity prior to collecting such data or information. It is worth noting here that this protection is available to all types of Personal Information, as covered by the 2011 Rules, and hence is also available to information or data other than that covered under sensitive personal data or information at par with the one which is so covered.[151]

(5) Withdrawal of Consent

Along with the prior mentioned right, the person from whom the information is sought also has the right to withdraw his consent which was earlier given. As a safeguard and to ensure that no

[151] Alan F Westin, "Science, Privacy and Freedom" 66 Columbia Law Review 1003 (1966)

one except the concerned person is withdrawing such consent, this withdrawal of consent id also required to be sent in writing.

(6) Information not to be retained for more than required time

Any person or entity who was retaining Sensitive Personal Data or Information is not permitted to retain such data or information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(7) Authorized Use of the Data or Information

As per the 2011 Rules, the information which is collected shall be used for only the purpose for which it has been collected and not otherwise.

(8) Permitting the Correction as well as Amended of the already provided information

Entity or the concerned person shall permit the persons by whom information was provided to review the information they had provided, as and when requested by them and shall ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.

(9) Keeping the Information secure in compliance with the 2011 Rules

Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

1.5 DISCLOSURE OF THE SENSITIVE PERSONAL INFORMATION OR DATA

The 2011 Rules under Rule 6 covers or encapsulates 3 methods whereby the disclosure of the Sensitive Personal Information is permitted, which will be discussed. As a caution, it is not to be confused with the "transfer of information' which is a different concept and will be addressed in the next heading. The 3 methods by which disclosure is permitted are :

(i) Disclosure to the third party by Prior Permission of the person who gave such information ;

(ii) Disclosure of Information to Government Agencies on certain grounds ;

(iii)Disclosure to the third party in compliance with an order passed under any law in force for the time being.

- ***By Prior Permission***

The Sensitive Personal Data or Information can be disclosed to any third party, provided that the person who has given such information has given his permission for such purpose. Such permission is not mandatorily required, for disclosing such information to the third party, if the information was shared under some sort of contract and that contract itself mentions that the parties agree to disclose such information. Another instance where such permission of the provider is not required is when the concerned person or the entity is under a legal obligation to do so.[152]

- ***Disclosure to Government Agencies***

Rule 6 of 2011 Rules provide certain situations wherein the Sensitive Personal Data or Information shall be shared with Government Agencies, even without asking for the permission of the provider of such information. The contingencies or situations under which the Government Agencies can obtain such data or information are:-

- for the purpose of verification of identity or
- for prevention, detection, investigation including cyber incidents or
- prosecution or
- Punishment of offences

Similar to this Rule 6 of 2011 Rules, Section 69 of the Information Technology Act, 2000, empowers the Central Government, State Government, and the persons specially authorized by Central or State Government in this behalf, to pass an order directing any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource, on any of the following grounds: -

- in the interest of the sovereignty or integrity of India ; or
- defense of India ; or

[152]Shrikant, Ardhapurkar&Srivastava, &Tanu, & Swati, Sharma &chaurasiya, Mr &Vaish, Abhishek. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. International Journal of Engineering Science and Technology 2

- security of the State ; or
- friendly relations with foreign States ; or
- public order ; or
- for preventing incitement to the commission of any cognizable offence relating to above ; or
- for investigation of any offence

- ***Disclosure to the third party under any law***

Rule 6 mentions that any Sensitive Personal Data or Information shall be disclosed to any third party by an order under the law for the time being in force.

1.6 TRANSFER OF INFORMATION

As mentioned above the disclosure of information is different from the transfer of information. In short, where disclosure is usually made to any person or entity which is independent from the one, the transfer is usually used when the information is exchanged between organizations or persons which are connected in a certain way.[153] Rule 7 of 2011 Rules, permits entity or authorized persons to transfer Sensitive Personal Data or Information, to any other body corporate or a person in India, or located in any other country, provided such intended recipient ensures the same level of data protection as provided for under the 2011 Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

1.7 FAILURE TO COMPLY WITH THE PROVISIONS

Since, 2011 Rules draw its powers from the IT Act 2000, there are certain provisions which provide for the contravention of certain provisions, and thus needs to be read for a better understanding of the concept at this point.[154]

[153] Privacy-Enhancing Technologies—approaches and development <http://www.sciencedirect.com/>
[154] Philip E. Agre, Marc RotenbergTechnology and privacy: the new landscape

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

Further ***Section 43A of the IT Act,*** relates to Compensation for failure to protect data. This provision applies to those body corporate which possess, deal or handle any Sensitive Personal Data or Information in a computer resource which it owns, controls or operates, and is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person. The provision provides that in the situation mentioned above, such body corporate shall be liable to pay damages by way of compensation to the person who is so affected.

1.8 POINTS TO BE PONDERED UPON

In the definition of Sensitive Personal Information under Rule 3 of 2011 Rules, certain information hasn't found a place which by their very nature are sensitive and needs to be adequately protected, and at par with information which has already been given security. In the last few years, reliance on the internet has increased rapidly at an exorbitant rate, and people who use internet usually put certain information which are sensitive but aren't protected by any legal frameworks from being misused.[155] Further, more and more people are joining and regularly using social networking websites, and are readily using electronic communication to be in touch with others. Thus, it is time to give a serious thought about whether electronic communicationrecords including emails, chat logs and other communications made using a computer do not need to legally protected against any possible misuse.

1.9 RECENT LEGAL UPDATES

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr v Union of India &Ors (W.P. (Civil) No. 494 of 2012),*** recognized and

<http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false>

[155] Data Protection Act 1998: 1998 CHAPTER29
<http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1>

pronounced the right to privacy as a fundamental right which is given under the Constitution of India. This landmark judgment definitely calls for an update of the Indian Laws in respect of the Information Technology as well.[156] To achieve this, Personal Data Protection Bill, 2018 was drafted and it is likely to be placed in the upcoming session of the Parliament by the Ministry of Electronics and Information Technology. The Bill intends to regulate the processing of personal data of individuals by government and private entities which are incorporated in India as well as those which are incorporated abroad. The Personal Data Protection Bill 2018, needs to address a lot of things which yet have not been discussed from a legal viewpoint and have been overlooked by the laws which have been in force till now. In the recent updates also, there has been news of government asking certain messaging apps like ***'Whatsapp'*** to share the data with the government authorities. It seems fair from one point, but on the other hand if we look at it from an individual's point of view, the invasion and sharing of chat details of an individual with anyone against or without his consent seems to be in direct conflict with his right to privacy, which as mentioned has been accorded the status of Fundamental Rights. Thus, the least we may expect of the Personal Data Protection Bill, 2018 is to address the issues and conflicts which have already arisen. The Bill in whatever manner passed will have a very big impact on the Information Technology in the upcoming years, and thus should also be far-sighted.

1.10 LET'S SUM UP

In this chapter, we have studied what is Sensitive personal data or information and personal information along with its legal definition. Furthermore, we studied the procedure to collect sensitive personal information and to whom the information has to be disclosed. Finally, we have ended our discussion with the recent legal updates with respect to sensitive personal data or information.

1.11 FURTHER READING

- Ijlljs.in (2019), http://ijlljs.in/wpcontent/uploads/2017/02/AN_ANALYSIS_OF_PERSONAL_DATA_P

[156] White Paper on Privacy Protection in India (Vakul Sharma) <http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf>

ROTECTION_WITH_SPECIAL_EMPHASIS_ON_CURRENT_AMENDMENTS_AND_PRIVACY_BILL.pdf (last visited Nov 20, 2019).

- Elplaw.in (2019), https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (last visited Nov 20, 2019).
- Webfoundation.org (2019), http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf (last visited Nov 20, 2019).
- Induslaw.com (2019), https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf (last visited Nov 20, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Define Personal Information?**

The definition of ***"Personal information"*** is found under ***Rule 2(i),*** it has been defined as, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

2. **Define Sensitive Personal Data or Information?**

Sensitive Personal Data or Information has been defined under ***Rule 3 of the 2011 Rules.*** It states that in respect of any person, the sensitive data or information is the one which consists of his information relating to:-

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details ;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;
vii. any detail relating to the above clauses as provided to body corporate for providing service; and

viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

3. **What is the punishment for failure to comply with the provisions related to disclosure of information?**

Section 72A of the IT Act, 2000 provides punishment for disclosure of information, knowingly and intentionally, without the consent of the person to whom the information relates, and in breach of the lawful contract as imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

4. **What is recent case law with respect to the right to privacy?**

The Hon'ble Supreme Court of India by its judgment in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr v Union of India &Ors (W.P. (Civil) No. 494 of 2012),*** recognized and pronounced the right to privacy as a fundamental right which is given under the Constitution of India.

1.13 ACTIVITY

Elaborate the procedure to collect Sensitive personal data or information and to whom the information must be disclosure along with the recent cases with respect to privacy issues? (1000-1500 words)

Unit 2: Laws related to Online Defamation

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Ingredients of Defamation

1.4 It all begins with publication

1.5 When?

1.6 How?

1.7 Where?

1.8 Who?

1.9 Online Defamation: An Indian Perspective

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The meaning of Defamation
- Ingredients of defamation
- Online Defamation: An Indian Perspective

1.2 INTRODUCTION

Defamation is defined as "an intentional false communication, either published or publicly spoken, that injuries another's reputation or good name." Defamation includes the common law

torts of libel (involving written or printed statements) and slander (involving oral statements). Significantly, both libel, as well as slander, could be committed via Internet medium.[157]

1.3 INGREDIENTS OF DEFAMATION

Defamation is an intrinsically personal wrong. The gist of defamation is actual or presumed damage to reputation flowing from publication.[158] In other words, defamation flows from publication (or communication) of information. In traditional libel cases "publication" is generally referred[159] to as "the date on which the libelous work was placed on sale or became generally available to the public". It has the following ingredients:

a) Publication of a statement;

b) The statement makes reference to the plaintiff;

c) Statement is communicated to some person or persons other than the plaintiff himself;

d) Statement reaches the plaintiff; and

e) Statement causes actual or presumed damage to the plaintiff.

The question is, does one encounter similar 'ingredients' when defamation occurs in Internet medium? Here, the only difference is that the tort of defamation occurs when the defamatory imputation is published in electronic form, everything else remains the same.

1.4 IT ALL BEGINS WITH PUBLICATION

Publication is defined as "the action of making publicly known". In the context of the Internet, the term publication includes dissemination, transmission and storage of information or data in electronic form.

In order to construe a relationship between defamation and publication in the Internet medium, one may have to answer the following questions:

[157]Biegel, Stuart, Beyond our Control – Confronting the limits of our Legal System in the Age of Cyberspace, MIT Press, London, [2003] at p 82

[158] M, Collins, The Law of Defamation and the Internet, Oxford University Press, [2001] p 24.02

[159]*Kenneth Love v William Morrow & Co.*, 193 AD 2d 583: 597 NYS 2d 424 2d Dep't. [1993]

1) When a "publication" takes place (which involves "time of occurrence");
2) How a "publication" takes place (which involves the "mode of publication");
3) Where the publication takes place (which involves issues such as "jurisdiction");
4) Who would be held responsible for the publication of the allegedly defamatory statements (ISP or the website promotor)?

1.5 WHEN?

Publication occurs when the contents of the publication, oral, spoken or written are seen and heard, and comprehended by the reader or hearer. From the point of view of the plaintiff, the process of publication is complete, when the communication reaches hi.

For example, In ***Godfrey vs Demon Internet Ltd.,***[160]the defendant ISP carried the newsgroup 'soc.culture.thai' and stored postings within that hierarchy for about a fortnight during which time the posting was available to be read by its customers. On 13 January 1997 someone unknown made a posting in the US in the newsgroup. This posting was squalid, obscene and defamatory of the plaintiff who was resident in England. On 17 January 1997 the plaintiff sent a letter by fax to the defendants, requesting them to remove the posting from their Usenet news server. The defendants could have obliterated the posting after receiving the plaintiff's request, but it remained available until its expiry on or about 27 January 1997. The plaintiff claimed damages for libel in respect of the posting after 17 January 1997 – the time when he affirmed to the ISP that the communication had indeed reached him.

Morland J. ruled:

"In my judgment, the defendant, whenever it transmits and whenever there is transmitted from the storage of its news server a defamatory posting, publish that posting to any subscriber to its ISP who accesses the newsgroup containing that posting. Thus every time one of the defendant's customers accesses 'soc.culture.thai' and sees that posting defamatory of the plaintiff, there is a publication to that customer".

[160]*Godfrey v Demon Internet Ltd,*4 All ER 342 (HC)

1.6 HOW?

How the publication has occurred, i.e., in what form (mode) publication has happened? It is an important issue in the techno-legal driven environment. It looks into the mode of publication (or transmission) – whether audio, video, textual or multimedia. Internet publishing is in 'electronic form'. Instances of defamation in 'electronic form' include generating, sending or receiving 'defamatory' e-mails, online bulletin board messages, chat room messages, music downloads, audio files, screaming videos, digital photographs etc. on the Internet.

1.7 WHERE?

Where the publication has occurred is not easy to define as a defamatory statement can be "published" anywhere in the world where there is access to the Internet. Here, the issue is whether due process of law would be served by hauling a defendant into a particular jurisdiction simply because he has posted information that can be accessed anywhere in the world.

In the context of Internet it is not necessary for the plaintiff in all cases to prove directly that the defamatory statement was brought to the actual knowledge of anyone (some person or persons other than the plaintiff himself), publication is only established if the plaintiff makes it a matter of reasonable inference that the publication was accessible in the said jurisdiction. In contrast, with the Internet, it is not at all probable that every website will be accessed in every jurisdiction where it can theoretically be accessed. So, as a matter of reasonable inference, it cannot be assumed that any site put on the Internet and theoretically accessible from anywhere is accessed everywhere. Where then can the publication be assumed to have taken place.

In ***R vs Graham Waddon,***[161] the defendant was charged with numerous counts of publishing obscene articles contrary to section 2(1) of UK's Obscene Publications Act, 1959. The defendant had created pornographic images, which were illegal under the UK's Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US-based Internet service provider. These images were accessible to anyone in the world via the Internet who became a subscriber

[161] *R v Graham Waddon* Southwark (Crown Court, 30-6-1999)

by giving credit card details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images. It was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore the instant court did not have jurisdiction.

Hardy, Christopher J. held:

"Publishing an article under Section 1(3)(b) of the 1959 Act included data stored electronically and transmitted. To transmit meant to send from one place or person to another. In the instant case, an act of publication took place when the data was transmitted by the defendant or his agent to the service provider, and the publication or transmission was in effect still taking place when the data was received. Both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving".

In other words, the court exercised its jurisdiction, even when the pornographic material was held on a US-based server. The court argument has been that since the material was uploaded (by Waddon) and downloaded (by the police) in the UK, it could be classified as being "published" in the UK.

In ***Dow Jones & Company IncvsGutnick,***[162] on the other hand, the High Court of Australia approved the trial court's assertion of jurisdiction over Dow Jones & Co., based on its online publication of an allegedly defamatory article. The article appeared in Barron's Online, the online version of Dow Jone's print publication Barron's, which was available to subscribers of wsj.com. Joseph Gutnick, a resident of the Australian state of Victoria, brought a defamation action against Dow Jones in a Victoria court. Dow Jones argued that the court should decline jurisdiction under the doctrine of forum non-conveniens, which would be applicable if the Victoria court was a "clearly inappropriate forum". Dow Jones argued that Barron's Online was published in New Jersey, the location of the servers hosting the wsj.com website. From this, it would follow that the substantive law to be applied in deciding the case in New Jersey law, which would make the Victorian court a inappropriate forum. Thus the decision hinged on where the article was deemed to be published.

[162]*Dow Jones & Company Inc vGutnick*[2002] HCA 56 (Austl)

The court held, contrary to Dow Jone's contention, that publication of a defamatory statement is "a bilateral act in which the publisher makes it available and a third party has it available for his or her comprehension". Therefore, the article was published, with respect to Gutnick's cause of action, not when Dow Jones placed it on its web server, but only when subscribers in Victoria accessed it. The site recorded about 550,000 hits, less than 0.01 percent of them from people with Australian credit cards. It was not ascertainable how many of these users were Victorian but it was agreed that "several hundred" downloads had taken place in Victoria. For these reasons, the court held that the defamation occurred in Victoria and that Victorian law-governed: "It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed". Since jurisdiction in Victoria was proper, and Victorian law would be applied, the Victorian court was not a "clearly inappropriate forum," and there was no basis for declining jurisdiction.

The court responded to Dow Jones's policy arguments with the observations: (1) a plaintiff can win damages only in a location where he has a reputation, which limits the choice of forum; (2) a judgment for damages is enforceable only in locations where the defendant has reachable assets; and (3) publishers can easily determine in advance which law will apply in defamation cases: the specter which Dow Jones sought to conjure up in the present appeal, of a publisher forced to consider every article it publishes on the World Wide Web against the defamation laws of every country from Afghanistan to Zimbabwe is seen to be unreal when it is recalled that in all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort.

The Court concluded for centuries that the law in defamation cases has been that publication takes place when and where the contents of the publication, oral or spoken, are seen and heard (i.e., made manifest to) and comprehended by the reader or hearer. Having decided that a person is defamed at the place where publication is made, the Court found that the dissemination of the material on the Internet and the downloading of that information in Victoria meant that publication had been made there.

1.8 WHO?

Who would be held responsible for the publication of the allegedly defamatory statements – the ISP or the website promoter? An Internet service provider represents an interactive network service. It may provide access to the Internet (a network of networks) only or offer a range of additional services. Depending upon its functional attributes, an Internet service provider may act as an 'information distributor (carrier)' or 'information publisher'.

An information distributor merely acts as a carrier of information (third party content) transmitting 'electronic message' from one place to another, without examining its content. The function of an information publisher is to not only publish and transmit the information but also take reasonable care in relation to the said publication.[163]

It is thus important to look into the cases, where the court has identified ISPs (or bulletin board operators) as either 'information distributor' or 'information publisher'. In ***Cubby, Incvs CompuServe, Inc.,***[164] where CompuServe is an online company providing access to over 150 special interest forums comprised of electronic bulletin boards, interactive online conferences, and topical databases. A newsletter called Rumorville was made available via the bulletin board. The plaintiff sued CompuServe for libel after allegedly defamatory statements were disseminated through the newsletter against it. Cubby argued that the court should consider CompuServe to be a "publisher" of the allegedly defamatory statements, and thus hold it liable for the statement.

1.9 ONLINE DEFAMATION: AN INDIAN PERSPECTIVE

In India, issue of defamation has so far been dealt under the provisions (Sections 499-502) of the Indian Penal Code, 1860. The Code makes no distinction between slander and a libel. It defines "defamation" as:

Section 499 states that, whoever by words, either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except[165] in the case hereinafter excepted, to defame that person.

[163]S KVerma and Raman Mittal (Ed.), Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, [2004], p 233

[164]*Cubby, Inc v CompuServe, Inc*776 F Supp 135 (SDNY) [1991]

[165] There are 10 exceptions (defences), that may be set up against a charge of defamation

The three ingredients[166] are:

1) Making or publishing any imputation concerning any person
2) Such imputation must have been made by
a) Words, either spoken or intended to be read; or
b) Signs; or
c) Visible representations
3) Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.

The Code also highlights that defamatory statements need to be published (or communicated). The Supreme Court held in ***Bennett Coleman & Co. vs Union of India,***[167] that "publication means dissemination and circulation". That is, communicating defamatory statements only to the person defamed is not publication.

It is important to note that an essential difference between the Indian and the English law is that the former recognizes 'words spoken' as a mode of defamation, and the latter does not. It was held by the Supreme Court in ***BalrajKhannavsMoti Ram:***[168]

"It will be highly desirable no doubt if the actual words stated to have been used by an accused and which are all to be defamatory are reproduced by the complainant. The actual words used or the statements made may be reproduced verbatim by the complainant if the words are few and the statement is very brief. But in cases where the words are spoken are too many or the statements made are too long, it will be the height of technicality to insist that the actual words and the entire statements should be produced verbatim".

The Code by highlighting that defamation could also happen by means of 'signs' or 'visible representations', has included every possible form of defamation, including defamation in 'electronic form' as well. Instances of defamation in 'electronic form' includes generating, sending or receiving 'defamatory' emails, messages, chat room messages, music downloads, audio files, streaming videos, digital photographs, tweets etc. on the Internet. Even sending

[166]Ratanlal and Dhurajlal, The Indian Penal Code, 28th Edn, P 686
[167]*Bennett Coleman & Co v Union of India*[1972] 2 SCC 788
[168]*BalrajKhanna vMoti Ram* AIR[1971] SC 1389

'defamatory' SMS, MMS, messages, photographs and videos on mobile phones would be considered instances of defamation in electronic form. In other words, the Code is sufficient in itself to tackle any online defamation matter. However, in ***ManikTanejavs State of Karnataka,***[169] it was held by the Supreme Court that:

"Facebook is a public forum; it facilitates the expression of public opinion. Posting of one's grievances against Government machinery, even on Government Facebook page does not by itself amount to criminal conduct".

Further, the Supreme Court in ***Subramanian Swamyvs Union of India,***[170] while examining the constitutional validity of Section 499 & 500 IPC has opined that "The decision in ***ShreyaSinghal case*** is placed reliance upon to highlight that a restriction has to be narrowly tailored, but criminal defamation is not a narrowly tailored concept".

1.10 LET'S SUM UP

In this chapter, we have studied the meaning and ingredients of defamation and the demarcation between defamation and online defamation. We also discussed how, when, and where online defamation commences. Finally, we ended the discussed with the Indian Perspective of Online defamation.

1.11 FURTHER READING

- Defamation on the Internet – a duty free zone after all? Uta Kohl, (2000) 22 Sydney L Rev 119, pp 126-27.
- Valdaya, Ankit, Legal Consequences of Online Defamation in India (January 28, 2014).
- Susan Singleton, Simon Halberstam, Business, The Internet And the Law, 1999, Tolley Publishers, U.K.
- Martin Samson, Online Defamation/Libel/Communications Decency Act - Internet Library of Law and Court Decisions

[169]Manik*Taneja v State of Karnataka* [2015] 7 SCC 423
[170]*Subramanian Swamy v Union of India*[2016] 7 SCC 221

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of defamation?

Defamation is defined as "an intentional false communication, either published or publicly spoken, that injuries another's reputation or good name."

2) What are the ingredients of defamation?

It has the following ingredients:

a) Publication of a statement;

b) Statement makes reference to the plaintiff;

c) Statement is communicated to some person or persons other than the plaintiff himself;

d) Statement reaches the plaintiff; and

e) Statement causes actual or presumed damage to the plaintiff.

3) What are the questions that need to be posed in order to find out the relationship between defamation and publication?

- When a "publication" takes place (which involves "time of occurrence");
- How a "publication" takes place (which involves the "mode of publication");
- Where the publication takes place (which involves issues such as "jurisdiction");
- Who would be held responsible for the publication of the allegedly defamatory statements (ISP or the website promotor)?

4) What are the ingredients of defamation as per IPC?

The three ingredients are:

a) Making or publishing any imputation concerning any person

b) Such imputation must have been made by

- Words, either spoken or intended to be read; or

- Signs; or
- Visible representations

c) Such imputation must have been made with the intention of harming or with knowledge or reason to believe that it will harm the reputation of the person concerning whom it is made.

1.13 ACTIVITY

Explain briefly the meaning and ingredients of defamation and how it is different from online defamation. Also, describe the same with relevant case laws as per the Indian perspective? (800-1000 words)

Unit 3: Body Corporate Responsibilities for Data Protection

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Legal definition of certain important terms

1.4 Responsibilities to be discharged by Body Corporate

1.5 Let's sum up

1.6 Further reading

1.7 Check your progress: Possible answers

1.8 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is meant by 'Reasonable Security Practices and Procedures'
- What are the responsibilities which need to be discharged by Body Corporates
- Can Body Corporates be held liable if the information given isn't authentic

1.2 INTRODUCTION

With the rampant use of the internet, there is an undeniable need for the protection of data that the people put up or share over the internet. This has been more firmly established by the pronouncement of judgment by the Honorable Supreme Court in the case of ***Justice K.S. Puttaswamy (Retd.) &Anr. v Union of India &Ors,***[171] which accorded the right of privacy as a fundamental right. Further, it is a recognized and a well-recognized jurisprudential principle that where there is a right, there is a duty. So in this situation, where the individuals have the right to privacy, the bodies or agencies which have the data of the individuals are under a duty to protect and restrain from the using or allowing the data to be used for any purpose other than that

[171] *Justice K.S. Puttaswamy (Retd) &Anr v Union of India &Ors* W P (Civil) No 494 of [2012]

permitted by law. In this chapter, we will focus on those duties of a body corporate that has been imposed upon them by the law with respect tothe protection of electronic data.

1.3 LEGAL DEFINITION OF CERTAIN IMPORTANT TERMS

The term ***'body corporate'*** has neither been defined under the Information Technology Act, 2000 nor under any of the Rules issued from time to time by the competent authorities which draw its validity and legal backing from the Information Technology Act 2000 (hereinafter referred to as 'the IT Act, 2000'). However, in the year 2008, certain provisions of the IT Act, 2002, were amended and amongst other provisions, ***Section 43A*** was brought in, which prescribed that the compensation has to be paid, to the provider of information, by the body corporate which possesses, deals or handles sensitive personal data or information who has a duty to implement and maintain reasonable security practices and procedures so as to prevent the information from unauthorized use, access, sharing, alteration or damage and which has failed to do so and, as a result of the unauthorized access or disclosure, certain loss has been caused. It is in the explanation part of this provision, certain terms have been defined, which sets out their meaning for the purpose of the section. It is in this part of this provision that body corporate has been defined. It states that 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

The term also defines ***'reasonable security practices and procedures'*** as those security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. Now, as the definition mentions the reasonable security practices and procedures as those practices as procedures as may be specified in law, the Central Government has framed certain Rules to regulate on these security practices and procedures drawing its validity under ***Section 43A and clause (ob) subsection (2) of Section 87 of the IT Act 2000.*** The Central Government notified these Rules in the year 2011, and they are ***called Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)***

Rules, 2011 (hereinafter referred to as 'the 2011 Rules'). Now we will look into the important amongst those guidelines. In the previous Chapter, those guidelines were discussed from the viewpoint of the provider of the information, but in this chapter, the discussion will follow the viewpoint of an organization that is collecting such information.

1.4 RESPONSIBILITIES TO BE DISCHARGED BY BODY CORPORATE

1. Responsibility of Body Corporate to provide a policy for privacy and disclosure of information.

   Under the 2011 Rules, ***Rule 4*** provides that the body corporate or any person, who on its behalf collects, receives, possess, stores, deals or handle information of provider of information, has to provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. Such body corporate or any person on its behalf shall ensure that such policy is available for seeing to such providers of information who has provided the concerned information under a lawful contract, and such policy shall be published online on the website of the body corporate. The policy shall have following things among others:-

   i. Clear and easily accessible statements of its practices and policies; and
   ii. Type of personal or sensitive personal data or information collected under Rule 3 of the 2011 Rules; and
   iii. Purpose of collection and usage of such information; and
   iv. Disclosure of information including sensitive personal data or information as provided in Rule 6 of the 2011 Rules;
   v. Reasonable security practices and procedures as provided under Rule 8 of the 2011 Rules.

2. As mentioned under ***Rule 5 of the 2011 Rules,*** it is duty or responsibility of the Body Corporate or the person working on its behalf to obtain the consent of the provider of the sensitive personal information or data. Such consent must be regarding the purpose of usage and must be obtained before the collection of such information.
3. It is also the responsibility of the body corporate or the person working on its behalf to endure that the provider of the sensitive personal information is aware that such information is being collected, and the purpose for which the information is being collected, and the intended recipients of the information sought to be collected, along with the name and

address of the agencies collecting the information and of those who will be retaining the information.[172]

4. The body corporate is also under an obligation to collect information only for a lawful purpose, which is connected with any activity or function of such body corporate and when the collection of information is necessary for that purpose.
5. The body corporate or the person acting on its behalf which is holding such sensitive personal information or data is under an obligation to not retain the information retained for any time longer than what is required for the lawful purpose for which the information was retained or than the period which is permitted under any law for the time being in force.
6. One of the most important and basic responsibilities of the body corporate or the person who is working on its behalf is that the information shall be used only for the purpose for which it was collected and nothing more. This responsibility restricts the body corporate from the misuse of the data collected and this is a very big onus being placed on the body corporate.
7. It is the duty of the body corporate to enable the data or information providers to correct or amend the data or information given by them, when they request for the same, and so far as this is feasible. The point worth noticing here is that the body corporate or the person working on its behalf isn't responsible for the correctness or the genuineness of the data or information given or corrected, as the case may be.
8. Another important obligation of the body corporate is that before collecting the information, it or any person working on its behalf shall provide the provider of the information with an option to not provide the concerned data or information.
9. The obligation mentioned in the point above is also available at a later stage, whereby the consent is given can be withdrawn at a later stage, and thereby the body corporate or any person working on its behalf shall be duty-bound not to use such data or information in respect of which the consent has been withdrawn.
10. Under sub-rule 5 of Rule 5 of the 2011 Rules, another responsibility of the body corporate has been encapsulated. This obligation or responsibility is that of grievance redressal of establishing an authority for the said purpose. The Rule states that the body corporate shall address any discrepancies and grievances of their provider of the information with respect to the processing of information in a time-bound manner. The Rule also mandates the body

[172] <https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>

corporate to designate a Grievance Officer, and to ensure that this is known to the people, it is obligated to publish his name and contact details online on its website. The Rule also prescribes a timeframe within which the grievances must be taken care of and mentions that the Grievance Officer shall redress the grievances or provider of information expeditiously but within 1 month from the date of receipt of the grievance.

11. Another obligation on the body corporate is mentioned in sub-rule 8 of rule 5 of 2011 Rules. It states that the body corporate or any person working on its behalf shall keep the information secure as provided in rule 8. In relation to the same, rule 8 talks about 'Reasonable Security Practices and Procedures.'

    Rule 8 talks about presumption, in favour of body corporate or person acting on its behalf, in respect of security practices and procedures provided that they have implemented such security practices and standards and have a comprehensively documented information security program and information security policies. The requirement of such policies shall contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[173]

    The rule further lists down certain standards which, if complied with, are sufficient to raise the presumption above mentioned.

    - One such standard is: The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements."
    - Any industry association or its entity, whose members are self-regulating by following any standard other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1) of Rule 8, needs to get its codes of best practices duly approved and notified by the Central Government for effective implementation.[174]

    The rule further mentions that the body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified (abovementioned) shall be deemed to have complied with reasonable security practices and procedures provided that such

[173]Rule 8: Reasonable Security Practices and Procedures <https://www.itlaw.in/rule-8-reasonable-security-practices-and-procedures/>

[174]<https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf>

standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource.

12. Regarding disclosure of information by the body corporate or any person working on its behalf, as the body corporate is responsible not to disclose the data or information to any other person or entity without the prior permission of the provider of the information, but this doesn't apply where the disclosure is a legal obligation of the body corporate.
13. In continuance of the obligation to not to disclose the information or data to any third party, another important yet interesting obligation of the body corporate is to disclose the data to the Government Agencies which are mandated under the law to obtain information which is covered under the 2011 Rules on certain grounds, and this has to be done by the body corporate without the prior permission of the provider of the information. So this rule is, in a way, an exception to the general rule that the disclosure of information can be made only after the prior permission of the provider. The grounds on which such disclosure is to be made by the body corporate to the Government Agencies include: for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. This rule, as mentioned in the one of the previous chapters is similar to one of the provisions under the IT Act which provides for similar grounds on which the governmental agencies can seek information from the entities retaining them and the latter are under an obligation to disclose the same to the concerned agencies on the orders of the authorities mentioned therein.[175]
14. Also, the disclosure of the information is mandatory for the body corporate in compliance with an order under the law for the time being in force (as per Sub-rule 2 of Rule 6 of 2011 Rules).[176]

[175]How to deal with Section 43A in a Company
<https://www.naavi.org/cl_editorial_12/edit_dec_2_sec43A_compliance_framework.html>
[176]Data Protected India | Insights | Linklaters
<https://www.linklaters.com/en/insights/data-protected/data-protected---india>

So these were the major responsibilities or obligations of the body corporate in respect of data protection, which can be ascertained from the legal regime which is existing at present.

1.5 LET'S SUM UP

In this chapter, we have studied the meaning of reasonable security practices and procedures along with certain important terms related to data protection. Finally, we have ended our discussion with the responsibilities to be discharged by body corporate.

1.6 FURTHER READING

- Privacyinternational.org (2019), https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf (last visited Nov 21, 2019).
- Ghosh, Dr. Jayanta. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.
- India: Data Protection & Cyber Security - AZB & Partners, AZB & Partners (2019), https://www.azbpartners.com/bank/india-data-protection-cyber-security/ (last visited Nov 21, 2019).
- Thelawreviews.co.uk (2019), https://thelawreviews.co.uk/digital_assets/25776d4c-702f-41bb-82a0-cb3e18240506/Privacy.pdf (last visited Nov 21, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Was 'body corporate' originally defined in the Information Technology Act, 2000?**
   No. However, Section 43A was inserted by Information Technology (Amended) Act, 2008, in the explanation of which the term 'body corporate' was defined for the first time in the law relating Information Technology.

2. **Can body corporate obtain information on the assumption that the provider of the information is aware of the purpose for which the information is to be used?**
   No, it has been mentioned under "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", that it is the responsibility of the body corporate to make sure that the provider of the information is aware of certain things, one of which is the purpose for which the information is being collected. And therefore the body corporate can't record the information or data on presuming the knowledge of the provider.

3. **Does body corporate need to obtain the prior permission of the provider of information if it is ordered to disclose the concerned information by a court's order?**

   In the situation mentioned above, since disclosing the concerned information becomes the legal obligation on the body corporate due to it coming from the court's order, hence the prior permission isn't necessary for such a situation.

4. **If the information is provided by a person with his free consent for a particular purpose, can such information be used for any other purpose for which he hasn't consented specifically?**

   The obligations as mentioned under the 2011 Rules, specify that the consent which is necessary must be for the specific purpose for which the information is to be used. Thus the information can't be used for any purpose other than that for which it was consented to.

5. **If the provider of the information has any grievance against any body corporate, whom does he need to approach, and by when shall the grievance be resolved?**

   The Body Corporate has to appoint a Grievance Officer for resolving such grievances, and it has to be done within one month.

1.8 ACTIVITY

Mention all the situations (covered under IT Act, 2000, and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011) under which the information or data can be disclosed to third parties. (800 Words)

Unit 4:Right To Be Forgotten

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Status of Right to be Forgotten vis-à-vis Right of Privacy: A thoughtful approach

1.4 Status of Right in the present Indian Legal Matrix

1.5 The birth of the Right to be forgotten

1.6 Judicial precedents framing the wat for the 'Right to be Forgotten' in India

1.7 The 2018 Bill and the Right to be forgotten

1.8 Shortcomings of the 2018 Bill

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The history of the right to be forgotten
- Approach of Indian Laws towards the concept of the right to be forgotten
- The Personal Data Protection Bill, 2018 in context of the right and its shortcomings

1.2 INTRODUCTION

The concept of the 'right to be forgotten' is very new and as of now, has legally found its mention only in the European Union. The best meaning which can be attributed to the term is the right of any person to restrain everyone else to publish or make known any information whatsoever regarding the former. In the Jurisprudence of Indian laws, the terms haven't been defined anywhere in any of the laws in force. However, there are certain provisions which prohibit the publishing of the names or any detail which could reveal the identity of a certain

person (majorly the rape victims). The recent and the most important thing in Indian Laws context is that the Ministry of Electronics & Information Technology under the Central Government has issued ***Personal Data Protection Bill, 2018 (hereinafter referred to as 'the 2018 Bill')***[177] which for the first time in the history of Indian Laws has dealt with the concept of the 'right to be forgotten', and that too in the field of Information Technology. This right in the form as in the 2018 Bill would be focused upon in this Chapter.

1.3 STATUS OF RIGHT TO BE FORGOTTEN VIS-À-VIS RIGHT OF PRIVACY: A THOUGHTFUL APPROACH

On a thoughtful consideration of the nature of the 'right to be forgotten', it would not be wrong to relate it with the right to privacy. To get a better understanding and to provide more clarity on the matter, let's look at it from the grass-root level. Suppose a person 'X' has provided certain information to the body corporate say 'Y', now assuming that 'X' hasn't been given the right to privacy under the laws by which he is being governed then obviously he wouldn't have the right to ask 'Y' to keep his data private and restrain from sharing it to anyone, which in essence is the whole foundation of the 'right to be forgotten' because the right is nothing more than the right to compel any person to either delete the data which he might have respecting a person or to delete such data, or in other words it is the right to ask the another to keep the information private, hence arising from the right of privacy only.[178]A very similar reasoning must have been followed in drafting the 2018 Rules, as is evident by reading the objectives to bring up the 2018 Bill. The Hon'ble Supreme Court has accorded the right to privacy a status of ***Fundamental Right, in the J. Puttaswamy case***[179]**.** Thus, it would be correct to say that the ruling, in that case, has paved the way for this right to be forgotten as well.

1.4 STATUS OF RIGHT IN THE PRESENT INDIAN LEGAL MATRIX

At present, the right to be forgotten, in whatever manner, in the present Indian laws can be ascertained by referring to certain provisions of ***Indian Penal Code, 1860 and Protection of***

[177]<https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>
[178] See EUROPEAN COMMISSION, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12) (2014),
<http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf>
[179][2017] 10 SCC 1

Children from Sexual Offences Act, 2012 and Juvenile Justice Act 2015. Looking at them individually as follows:

- Under Indian Penal Code, Section 228A, prevents any person from making known the name and identity of the victim of offences falling under 376, 376A, 376AB, 376B, 376C, 376DA, 376DB or 376E, by making it an offence to do so.
- Under the Protection of Children from Sexual Offences Act, 2012, a combined reading of Section 24(5) and Section 33(7) makes it sufficiently apparent that the name and identity of the child are not to be disclosed at any time during the course of investigation or trial.
- Under the Juvenile Justice Act, 2015, the proceedings against any juvenile are required not to be recorded. This is directed with an intention to prevent the identity of such juvenile known from others.

1.5 THE BIRTH OF THE RIGHT TO BE FORGOTTEN

For understanding more clearly the importance of the right, it would be helpful to read about the journey of the same.

- The origin of ***'Right to be Forgotten'*** can be traced back to the western countries in the year 1995. Back then, the European Union brought in force their first-ever piece of law in the field of personal data protection, which is ***'Directive 95/46/EC'.*** It is important to note that the said document didn't specifically mention the term "right to be forgotten" but the same was readily inferable when ***Article 6(1)(e) is read with Article 12(b).*** Where the prior provision refrains the data from being used for any purpose other than the one for which it was collected, whereas the latter gave the provider of the information the right to ask to rectify, erase or block the data which is found violative of this Directive 95/46/EC.
- Later, the 'Right to be Forgotten' was laid down by the European Court of Justice in the case of ***Google Spain SL v. Agencia Española de Protección de Datos& Mario Costeja Gonzalez (famously known as the "Google Spain Case").*** In the case, the European Court of Justice upheld the 'Right to be Forgotten' if the data related to him is not needed for the purpose for which it was collected.[180]

[180] RAYMOND S.R. KU & JACQUELINE D. LIPTON, CYBERSPACE LAW: CASES AND MATERIALS 117 (3rd ed. 2010)

- Then in the year 2016, ***the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as 'the GDPR')*** was drafted which came into force from 2018. It is a regulation on data protection and privacy. Under Article 17 of the GDPR individuals have the right to have personal data erased, it is this right which is also known as the 'right to be forgotten'. It has to be noted that this right is not absolute and only applies in certain circumstances. With the coming in force of the GDPS, the 'Directive 95/46/EC' has been repealed.[181]

1.6 JUDICIAL PRECEDENTS FRAMING THE WAY FOR THE 'RIGHT TO BE FORGOTTEN' IN INDIA

The 'Right to be Forgotten' as mentioned earlier isn't found on any of the laws in India, not even in the Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011. However, there are certain judicial pronouncements on the matter. The Gujarat High Court and the Karnataka High Court have taken differing stands on the 'Right to be Forgotten'. Gujarat High Court in ***DharamrajBhanushankar Dave v. State of Gujarat &Ors.***[182]denied to recognize any such right. In this case, the respondent had published a non-reportable judgment on a website which concerned the plaintiff as well, and the High Court in its judgment refused to compel the respondent to take the same down. The High Court then held that the petitioner failed to prove any violation of ***Article 21 of the Constitution of India.*** The analysis of this judgment gives an idea that the Gujarat High Court did not recognize the 'Right to be Forgotten'.

However, the Karnataka High Court in the case of ***Sri Vasunathan v. The Registrar General &Ors.***[183]recognized the 'Right to be Forgotten'. In the judgment, the High Court directed the respondent to remove the name of plaintiff's daughter as the High Court had earlier quashed the FIR against her by an order. ***Justice AnandByrareddy*** who gave the judgment in the case opined that:

"This would be in line with the trend in the Western countries where they follow this as a matter of rule "Right to be Forgotten" in sensitive cases involving women in general and

[181]Frosio, Giancarlo (2017) Right to Be Forgotten: Much Ado About Nothing. SSRN Electronic Journal. 10.2139/ssrn.3009153
[182]*DharamrajBhanushankar Dave v State of Gujarat &Ors*SCA No 1854 of [2015]
[183]*Sri Vasunathan v The Registrar General &Ors* W P No. 62038/2016

highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."

Apart from these judgments, another important order is the order of the Delhi High Court, in the case of ***ZulfiqarAhman Khan v. Quintillion Business Media Pvt. Ltd.***[184] In this case, the plaintiff was accused in ***#MeToo complaints*** and the respondents published a couple of article regarding the same which were ordered by Delhi High Court to be taken down and the court also ordered these articles not to republished by any other person also. However, another platform published those articles and thus on this issue, the court passed an order restraining the re-publication of the said articles till the time matter is pending in the Court. The Delhi High Court also said that the ***'Right to be Forgotten'*** as well as ***'Right to be Left Alone'*** are the inherent facets of ***'Right to Privacy'.***[185]

1.7 THE 2018 BILL AND THE RIGHT TO BE FORGOTTEN

Before coming to the discussion of the 2018 Bill, it is important to look at certain definitions, which will be helpful in the discussion below.

- ***Section 3(14) of the 2018 Bill,*** defines ***'Data Principal'*** as "natural person to whom the personal data referred to in sub-clause (28) relates".
- ***Section 3(13)of the 2018 Bill,*** defines ***'Data Fiduciary'*** as "any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of the processing of personal data"

The 'Right to be Forgotten' is not a settled and recognized concept of law in India but it has been incorporated under the newly drafted 2018 Bill. Section 27 of the 2018 Bill encapsulates the 'Right to be Forgotten'. It gives 'data principal' a right to restrict the disclosure of his/ her personal data by 'data fiduciary'. The Section also provides that the 'data principal' shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal on the grounds if:

(a) his personal data has served the purpose for which it was collected; or

(b) he withdraws his consent for collecting his personal data; or

[184] *ZulfiqarAhman Khan v Quintillion Business Media Pvt. Ltd* CS (OS) 642/2018

[185] <https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf>

(c) the disclosure of his personal data is in violation of any existing legislation.

However, this right would be given effect to if and when the Adjudicating Officer is satisfied that the said right overrides the Right to Freedom of Speech and Expression and the Right to Information of other citizens of India.

The next provision which relates to the matter in hand is Section 10 of the 2018 Act. It is well accepted that the 'Right to be Forgotten' does not include in itself the right to deletion of the data but Section 10 of the 2018 Bill places the obligation on 'data fiduciary' to delete the personal data which was collected, after the time during which it may reasonably be necessary for the purpose for which such data was collected. However, it may extend the abovementioned time, if the retention of the data is made any legal obligation. A careful reading of the 2018 Bill shows the intention of the 2018 bill to point out that the deletion of personal data is not a matter of right for 'data principal' but it's an obligation on 'data fiduciaries'.

Another unique feature which has been attached in exercise of 'Right to be Forgotten' under the 2018 Bill is that before the exercise of this right, an application has to be filed by the 'data principal' before the Adjudicating Officer. This is unique feature attached with this right, because such application needn't be filed before exercising any of the other rights available to 'data principal'. This feature has undoubtedly made the exercise of this right relatively time consuming.

1.8 SHORTCOMINGS OF THE 2018 BILL

Few of the shortcomings of the 2018 Bill, which can be found out are:

1. 'Right to be Forgotten' can't be given the status of an absolute right as it will do more harm than good. Under the GDPR, there is a bar on exercise of right the if the data is needed for the purpose of public interest, compliance with any legal obligation, national security, scientific and historical research etc. On the other hand, under the 2018 Bill, the restriction of the exercise of the right is given on the grounds of 'right to freedom of speech and expression' and the 'right to information' of any citizen. Thus in 2018 Bill, it

is evident that the grounds of the restrictions in the exercise of the right are narrower and do not cover other important grounds like those covered under the GDPR.[186]

2. Also, the exercise of this right in its true sense may also involve the deletion of information from private storage which isn't practically feasible and also might create a hurdle in publishing the information later on. Thus, a distinction between the deletion of information and restriction over disclosure of information would be more appropriate, and only the latter one is more feasible to be granted.
3. Under the 2018 Bill, there is a very apparent confusion about the ownership of the personal data. Regarding the deletion of the data, the 'data principal' has to apply before the Adjudicating Officer, and hence here the discretion is given to such officer, this impliedly refutes the point that the owner of the data is the 'data principal'. Further, Section 27 of the 2018 Bill gives the right to apply before review even to third parties, thus this provision also adds on to the confusion over the ownership of the data.
4. Under Section 28(2) of the 2018 Bill, 'data fiduciary' is empowered to charge a reasonable fee for complying with the request of, and, when any 'data principal' exercises the rights granted to him under the PDP Bill. The provision seems fine but the problem with it is that there is nothing in the 2018 Bill to fix the criteria for determining such fee. Such uncontrolled power is susceptible of being misused by the 'data fiduciary'.

The Bill is still a draft and hasn't been codified into an Act yet, and any shortcomings can be taken care of right now. Introducing the same changes later on would be more difficult once the Bill takes the form of an Act, and thus the concerned ministry and policy makers must take up the suggestions which have been sent in huge numbers and must incorporate the best ones so as to obtain a law which, though is certain to be a landmark but, must be such that the other nations also must look up to as an ideal law in the field.

1.9 LET'S SUM UP

In this chapter, we have studied the history of the right to be forgotten along with the status of Right to be Forgotten vis-à-vis Right of Privacy. Furthermore, we studied about the approach of Indian Laws towards the concept of the right to be forgotten. Finally, we have ended our discussion with the Personal Data Protection Bill, 2018 and the shortcomings of the bill.

[186]<https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf>

1.10 FURTHER READING

- Article19.org (2019), https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf (last visited Nov 22, 2019).
- Myers, Marcus. (2014). Digital Immortality vs. "The Right to be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy. Romanian Journal of Communication and Public Relations. 16. 10.21018/rjcpr.2014.3.175.
- Frosio, Giancarlo. (2017). Right to Be Forgotten: Much Ado About Nothing. SSRN Electronic Journal. 10.2139/ssrn.3009153.
- Scholarlycommons.law.case.edu (2019), https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1081&context=jolti (last visited Nov 22, 2019).

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Whether the 'Directive 95/46/EC' categorically recognized Right to be forgotten?**
   No. the first time this right was categorically recognized was in General Data Protection Regulation (EU) 2016/679.

2. **Whether any person can apply for the exercise of right to be forgotten?**
   No. Only the 'data principal' is entitled to apply before Adjudicating Officer for the exercise of the right dealt with under section 27 of the 2018 Rules.

3. **What are the grounds under which the 'data principal' can ask for his right mentioned under Section 27 of the 2018 Bill?**
   The grounds on which the 'data principal' can ask for exercise of his right to be forgotten are as follows:

   (a) his personal data has served the purpose for which it was collected; or

   (b) he withdraws his consent for collecting his personal data; or

   (c) the disclosure of his personal data is in violation of any existing legislation.

4. **When can Adjudication Officer refuse the 'data principal' from exercising his right under Section 27 of the 2018 Bill?**

Adjudication Officer may refuse the 'data principal' from exercising the mentioned right if the rights and interests of the 'data principal' in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen.

5. **Whether Section 228A of the Indian Penal Code, 1860, protects from disclosure the identity of the person accused of Section 377 of the IPC?**

   No, since Section 228A of the IPC specifically enlists certain provisions, and the details as to the identity of the person who are victims of those mentioned provisions only is prohibited, and Section 377 of IPC isn't one of those provisions thus it won't be covered under Section 228A of IPC. Moreover, the identity of the victims is being shielded under sections 228A and not of those who are perpetrators.

1.12 ACTIVITY

Write a note on whether the right to be forgotten shall supersede the right to know along with relevant legal backing. Also, if supporting the harmonious approach, also suggest the approach which you think would best suit the conditions of our country. (1000-1500 words)

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-949119-9-9

Dr.Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-104

Digital Records and Cyber Forensics

Post Graduate Diploma in Cyber Law (PGDCL)

2020

Digital Records and Cyber Forensics

Dr. Babasaheb Ambedkar Open University

Digital Records and Cyber Forensics

Course Writer

Mr.Yogesh Thandge — Cyber Forensic Analysts & Independent Consultant,Pune, Maharashtra

Dr.Deesha Khaire — Assistant Professor (Law), Gujarat National Law University, Gandhinagar, Gujarat

Content Editors

Prof. (Dr.) Nilesh K. Modi — Professor & Director, School of Computer Science
Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. June 2020

This publication is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) https://creativecommons.org/licenses/by-nc-sa/4.0/

ISBN: 978-81-949119-2-0

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr. Babasaheb Ambedkar Open University

PGDCL-104

Digital Records and Cyber Forensics

Block-1: INTRODUCTION TO FORENSIC CONCEPTS

UNIT-1 BASICS OF FORENSIC CONCEPTS 006

UNIT-2 OVERVIEW OF DIGITAL RECORDS AND CYBER FORENSICS 026

UNIT-3 INVESTIGATION PROCESS 041

UNIT-4 ELECTRONIC DISCOVERY: AN INTRODUCTION 054

Block-2: CYBER FORENSICS PROCESS, STANDARDS AND CHALLENGES

UNIT-1 DIGITAL EVIDENCE AND PROCESSES INVOLVED IN DIGITAL FORENSICS 066

UNIT-2 OVERVIEW OF FIRST RESPONDER 078

UNIT-3 EVIDENCE MANAGEMENT AND ANTI-FORENSICS 096

UNIT-4 NETWORK INVESTIGATIONS 112

Block-3: ROLE AND ANALYSIS OF CYBER FORENSICS

UNIT-1 COMPUTER FORENSICS AND ITS SIGNIFICANCE 124

UNIT-2 WINDOWS FORENSIC ANALYSIS 133

UNIT-3 DATA RECOVERY FUNCTION TESTING FOR DIGITAL FORENSIC TOOLS 144

UNIT-4 AVENUES FOR PROSECUTION AND GOVERNMENTS EFFORTS 154

Block-4: CYBER FORENSICS FROM LAW ENFORCEMENT PERSPECTIVE

UNIT-1 COMPUTER FORENSICS AND THE PROCESS OF CONFISCATION 167

UNIT-2 RELEVANCE OF INDIAN EVIDENCE ACT TO CYBER FORENSICS 180

UNIT-3 CYBER FORENSIC LABS AND CHALLENGES BEFORE LAW ENFORCEMENT AGENCIES 192

UNIT-4 MOBILE NETWORK INVESTIGATIONS 206

Block-1
Introduction to Forensics Concept

Unit 1: Basics of Forensic Concepts

1

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Evolution of Computer Forensics
1.4 Objectives of Computer Forensics
1.5 Basic Concept of Computer Forensics
1.6 Uses of Computer Forensics
1.7 Ethics to be followed by Digital Forensics Expert
1.8 Implications of Digital Forensics
1.9 Computer Forensics Investigation Process
1.10 Let's sum up
1.11 Further reading
1.12 Check your progress: Possible answers
1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Evolution of Computer Forensics
- Scope of Cyber Forensics
- Investigation process

1.2 INTRODUCTION

The advancement of Information and Communication Technologies (ICT) opens new avenues and ways for cybercriminals to commit crime. The recent development in Information Communication Technology (ICT) has made tremendous changes in every aspect of our life. These changes have been clearly reflected in cyberspace-related areas.[1] Cybercrime describes a wide range of circumstances in which technology is involved in the commission of a crime. It presents numerous and constantly evolving challenges to government and law enforcement. Cybercrime is an umbrella term used to describe two distinct but closely related criminal activities i.e., ***Cyber-dependent and Cyber-enabled crimes.*** The former are offences that can only be committed by using a computer, computer networks, or another form of ICT. These acts include the spreading of viruses and other malicious software and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, Cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another form of ICT.

Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. It deals with the preservation, identification, extraction and documentation of computer evidence. Like many other forensic sciences, computerforensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. The use of specialized techniques for recovery,authentication, and analysis of computer data, typically of data which may have been deletedor destroyed.[2]

Digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating

[1]"Bridging the gap in Legislation, Investigation
<https://vc.bridgew.edu/ijcic/vol2/iss1/5/>
[2]Cybercrime and Digital Forensics: Bridging the gap
<https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1014&context=ijcic>

or furthering the reconstruction of events found to be criminal; or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

1.3 EVOLUTIONS OF COMPUTER FORENSICS

The field of Computer Forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. The fields of information security which focuses on protecting information and assets, and computer forensics, which focuses on the response of hi-tech offenses, started to intertwine. The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents. In 1892, a eugenicist named Sir Francis Galton established the first system for classifying fingerprints. Sir Edward Henry, the commissioner of the Metropolitan Police of London, developed his own system in 1896 based on the direction, flow, pattern and othercharacteristics in fingerprints.[3] The Henry Classification System became the standard forcriminal fingerprinting techniques worldwide.The timeline of the evolution of computer forensics are as follows:-

YEAR	EVENT
1835	Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to murder weapon. Later, a team of scientists at the Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1836	James Marsh developed a chemical test to detect arsenic, which was used during the murder trial.
1892	Sir Francis Galton established the first system for classifying fingerprints.
1896	Sir Edward Henry, based on the direction, flow, pattern and other characteristics in

[3] Richard III GG, Roussev V Next-generation digital forensics. Communications of the ACM 2006 Feb 1;49(2):76-80

	fingerprints.
1920	American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings.
1930	Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups.
1970	Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1984	FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.
1988	International Association of Computer Investigative Specialists (IACIS) was formed.
1995	International Organization on Computer Evidence (IOCE) was formed.
1997	G8 nations declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".
1998	- G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. - 1st INTERPOL Forensic Science Symposium was held.
2000	First FBI Regional Computer Forensic Laboratory was established.

1.4 OBJECTIVES OF COMPUTER FORENSICS

The objectives of Computer forensics are to provide guidelines for:[4]

- Following the first responder procedure and access the victim's computer after the incident.

[4] Rogers MK, Seigfried K The future of computer forensics: a needs analysis survey Computers & Security. 2004 Feb 29;23(1):12-6

- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

1.5 BASIC CONCEPT OF COMPUTER FORENSIC

Regardless of specific case or technology used, the concept of computer forensics is constant and consists of four basic steps which include:

- ***Preparation***

Preparation includes understanding local laws, legal issues and determination of tools and procedures to employ in carrying out computer forensics tasks. This step also includes understanding the assignment at hand, preparing the team, and checking equipment.

- ***Collection***

This involves on-site acquisition of digital evidence by making binding copy of hard drives and learning the unusual or evidence collection and taking the collected evidence to the laboratory where evidence acquisition is made. Another method of collection is live forensics when evidence is collected from powered-on computers.

- ***Examination and Analysis***

This is a key area of computer forensics and involves examination of data, internet artefacts, temporary files, spool files, shortcuts, keywords search and dealing with encryption.

- ***Reporting***

This involves a court expert report being made according to valid templates. The reports are written the way the judges and prosecutors understand it.[5]

1.6 USES OF COMPUTER FORENSICS

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

Computer forensics is used in a variety of cases such as:-

- Intellectual Property Theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the workplace
- Regulatory compliance

[5]Prasanthi, B. V. "Cyber Forensic Tools: A Review" International Journal of Engineering Trends and Technology (IJETT) 41.Number-5 (2016): 6

1.7 ETHICS TO BE FOLLOWED BY DIGITAL FORENSICS EXPERT

Digital Forensic expert is an investigator that investigates the digital evidence. The task of the Digital Investigator is very crucial as any information left can lead the case in a different situation.[6] So some ethics are expected to be followed by the Digital Investigator while conducting the investigation such as:

- The investigator should not delete or alter any evidence i.e., any proof related to the case should be kept at secure place and should not be damaged.
- Should protect the computer/digital devices against viruses viz-a-viz viruses should be removed so that they don't destroy any information.
- Keep a log of all work done.
- Keep any Client Attorney information that is gained confidential.

The role of Digital Investigator in a Forensic investigation of a crime is complicated which starts at the crime scene, continues into the computer labs for deep investigation, and ends in the court where the final judgment is done. There is no scope of negligence at all.

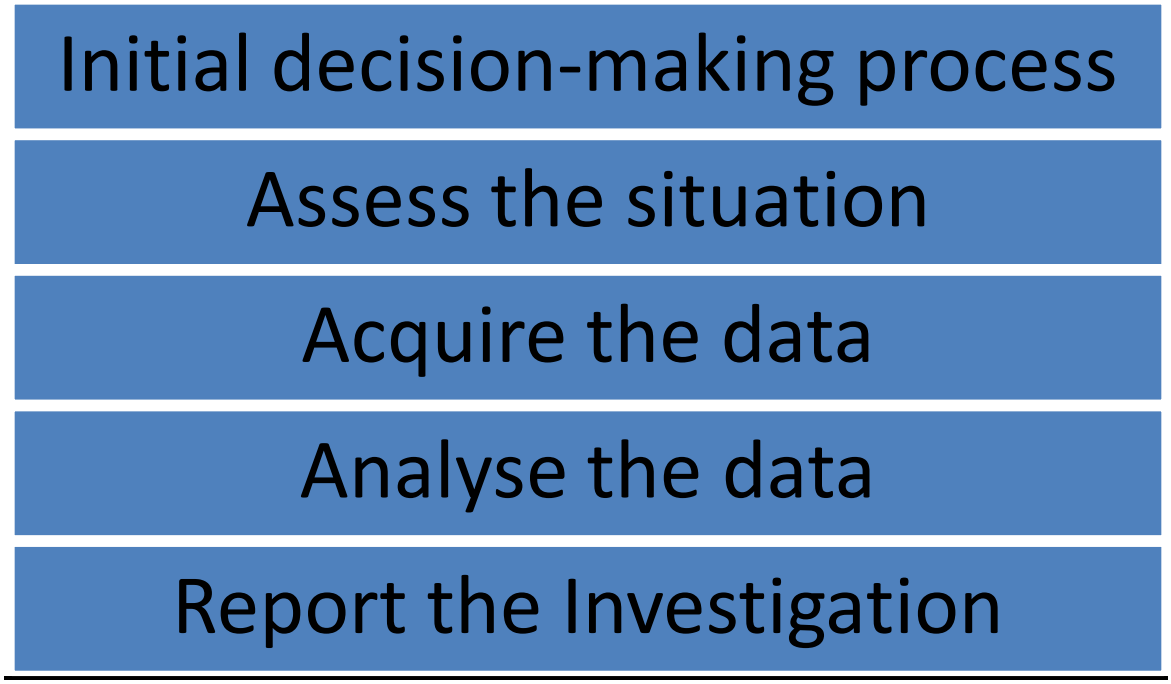
1.8 IMPLICATIONS OF DIGITAL FORENSICS

Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings.[7] As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate

[6]Sekar, Vyas, et al "Toward a framework for internet forensic analysis." ACM HotNets-III 2004
[7]Prasanthi, B V (2017). Cyber Forensic Science to Diagnose Digital Crimes- A study. International Journal of Computer Trends and Technology (IJCTT)

investigations.The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actusreus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.9 COMPUTER FORENSICS INVESTIGATION PROCESS



The investigation process of computer forensics are as follows:-

- **INITIAL DECISION-MAKING PROCESS**

  One must determine whether or not to involve law enforcement with the assistance of legal advisors. If the determination of law enforcement is needed, then the internal investigation must continue unless law enforcement officials advise otherwise. Depending on the type of incident being investigated, the primary concern should be to prevent further damage to the

organization by those person(s) who caused the incident. The investigation is important but is secondary to protecting the organization unless there are national security issues.[8]

- **ASSESS THE SITUATION**

The assessment of situation establishes the required resources for an internal investigation. There is a five-step process that must be followed which is as follows:-

a) Notify decision-makers and acquire authorization

To conduct a computer investigation, one must first need to obtain proper authorization unlessexisting policies and procedures provide incident response authorization. One must need to conduct a thorough assessment of the situation and define a course of action. The following are some of the best practices:

- If no written incident response policies and procedures exist, notify decision-makers and obtain written authorization from an authorized decision-maker to conduct the computer investigation.

- Document all actions you undertake that are related to this investigation. Ensure there is a complete and accurate documented summary of the events and decisions that occurred during the incident and the incident response. This documentation may ultimately be used in court to determine the course of action that was followed during the investigation.[9]

- Depending on the scope of the incident and absent any national security issues or life safety issues, the first priority is to protect the organization from further harm.

[8] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016

[9]What Is Computer Forensics? (GUIDE) | Forensic Control <https://www.forensiccontrol.com/what-is-computer-forensics>

After the organization is secure, restoration of services (if needed) and the investigation of the incident are the next priorities.

Decisions made may be questioned as much as the evidence. Because computer evidence is complex, different investigations (such as those conducted by an opposing party) may make different decisions and reach different conclusions.

b) Review policies and laws

At the start of a computer investigation, it is important to understand the laws that might applyto the investigation as well as any internal organization policies that might exist. The following are the best practices:-

- Determine if you have the legal authority to conduct an investigation. Many organizations state in their policies and procedures that there is no expectation of privacy in the use of the organization's equipment, e-mail, Web services, telephone, or mail and that the company reserves the right as a condition of employment to monitor and search these resources. Such policies and procedures should be reviewed by the organization's legal advisors, and all employees, contractors, and visitors should be notified of their existence. If you are uncertain about your authority, contact your management, your legal advisors, or (if necessary) your local authorities.
- Consult with legal advisors to avoid potential issues from improper handling of the investigation.[10] These issues may include:

    - Compromising customers' personal data.
    - Violating any state or federal law, such as federal privacy rules.
    - Incurring criminal or civil liability for improper interception of electronic communications. Consider warning banners.

[10] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

- Viewing sensitive or privileged information. Sensitive data that may compromise the confidentiality of customer information must only be made available as part of investigation-related documentation if it directly pertains to the investigation.

- Maintain digital copies of evidence, printouts of evidence, and the chain of custody for all evidence, in case of legal action. Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence when they handled it, and the locations, dates, and times of where the evidence was stored. Secure storage of evidence is necessary, or custody cannot be verified.

c) Identify Investigation Team Members

Ideally, team members should be established before the team is needed for an actual investigation. It is important that investigation teams be structured appropriately and have appropriate skills. The following are the best practices for forming an investigation team:-

- Identify a person who understands how to conduct an investigation. Remember that the credibility and skills of the person performing the investigation are often scrutinized if a situation results in legal proceedings in a court of law.
- Identify team members and clarify the responsibilities of each team member.
- Assign one team member as the technical lead for the investigation. The technicallead usually has strong technical skills and is experienced in computer investigations. In investigations that involve suspected parties who are technicallyskilled, you might need to select investigation team members who are more skilled than the suspected parties.
- Keep the investigation team as small as possible to ensure confidentiality and toprotect your organization against unwanted information leaks.
- Engage a trusted external investigation team if your organization does not have personnel with the necessary skills.

- Ensure that every team member has the necessary clearance and authorization toconduct their assigned tasks. This consideration is especially important if any third-party personnel, such as consultants, are involved in the investigation.[11]

d) Conduct a thorough assessment

Clearly documented assessment of the situation is required to prioritize your actions and justify the resources for the internal investigation. This assessment should definethe current and potential business impact of the incident, identify affected infrastructure, and obtain as thorough an understanding as possible of the situation. This information will help you define an appropriate course of action. The following are the best practices to conduct a thorough assessment:-

- Use all available information to describe the situation, its potential severity, potentially affected parties, and (if available) the suspected party or parties.
- Identify the impact and sensitivity of the investigation on your organization. For example, assess whether it involves customer data, financial details, health care records, or company confidential information. Remember to evaluate its potentialimpact on public relations. This assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.
- Analyse the business impact of the incident throughout the investigation. List thenumber of hours required to recover from the incident, hours of downtime, cost of damaged equipment, loss of revenue, and value of trade secrets. Such an assessment should be realistic and not inflated. The actual costs of the incident willbe determined at a later date.
- Analyse affected intangible resources, such as the future impact on reputation, customer relationships, and employee morale. Do not inflate the severity of the incident. This analysis is for informational purposes only to help understand the scope of the incident. The actual impact will be determined at a later date. This

[11] Barrett, Neil, Computer Forensics Jump Start: Computer Forensics Basics, Solomon, Sybex Printing, 2005

assessment will likely be beyond the expertise of IT and should be done in conjunction with management and legal advisors.

e) Prepare for Evidence Acquisition

A detailed document containing all information must provide a starting point for the next phase and for the final report preparation. In addition, understand that if the incident becomes more than just an internal investigation and requires court proceedings, it is possible that all processes used in gathering evidence might be used by an independent third party to try and achieve the same results. The document that provides detailed information about the situation and must include the following:-

- An initial estimate of the impact of the situation on the organization's business.
- A detailed network topology diagram that highlights affected computer systems and provides details about how those systems might be affected.
- Summaries of interviews with users and system administrators.
- Outcomes of any legal and third-party interactions.
- Reports and logs generated by tools used during the assessment phase.
- A proposed course of action.

- **ACQUIRE THE DATA**

Somecomputer investigation data is fragile, highly volatile, and can be easily modified or damaged.Therefore, one needs to ensure that the data is collected and preserved correctly prior toanalysis. There is a three-step process that must be followed which is as follows:-

a) Build computer investigation toolkit

A toolkit might contain a laptop computer with appropriate software tools, operating systems and patches, application media, write-protected backup devices, blank media, basic networking equipment, and cables. Ideally, such a toolkit will be created in advance, and team members will be familiar with the tools before they have to conduct an

investigation.The following are the guidelines that needs to be followed when building and using a computer investigation toolkit:-

- Decide which tools you plan to use before you start the investigation. The toolkit will typically include dedicated computer forensics software, such as Sysinternals, Encase, The Forensic Toolkit (FTK), or ProDiscover.
- Ensure that you archive and preserve the tools. You might need a backup copy of the computer investigation tools and software that you use in the investigation to prove how you collected and analysed data.
- List each operating system that you will likely examine, and ensure you have the necessary tools for examining each of them.
- Include a tool to collect and analyse metadata.
- Include a tool for creating bit-to-bit and logical copies.
- Include tools to collect and examine volatile data, such as the system state.
- Include a tool to generate checksums and digital signatures on files and other data, such as the File Checksum Integrity Validator (FCIV) tool.
- If you need to collect physical evidence, include a digital camera in the toolkit.

b) Collect the data

Data collection of digital evidence can be performed either locally or over a network. Acquiring the data locally has the advantage of greater control over the computer(s) and datainvolved. However, it is not always feasible. Other factors, such as the secrecy of the investigation, the nature of the evidence that must be gathered, and the timeframe for the investigation will ultimately determine whether the evidence is collected locally or over the network.

c) Store and archive

When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity. The best practices for data storage and archival include the following:-

- Physically secure and store the evidence in a tamper-proof location.
- Ensure that no unauthorized person has access to the evidence, over the network orotherwise. Document who has physical and network access to the information.
- Protect storage equipment from magnetic fields. Use static control storage solutions toprotect storage equipment from static electricity.
- Make at least two copies of the evidence you collected, and store one copy in a secureoffsite location.
- Ensure that the evidence is physically secured as well as digitally secured.
- Clearly document the chain of custody of the evidence. Create a check-in / check-outlist that includes information such as the name of the person examining the evidence,the exact date and time they check out the evidence, and the exact date and time they return it.

- **ANALYSE THE DATA**

There is a three step process to analyse the evidence that is gathered during the acquisition of data phase of an internal investigation.

a) Analyse network data

When network analysis is required, the following procedure is followed:-

- Examine network service logs for any events of interest. Typically, there will be large amounts of data, so you should focus on specific criteria for events of interest such as username, date and time, or the resource being accessed.
- Examine firewall, proxy server, intrusion detection system (IDS), and remote access service logs. Many of these logs contain information from monitored incoming and outgoing connections and include identifying information, such as IP address, time of the event, and authentication information.

- View any packet sniffer or network monitor logs for data that might help you determine the activities that took place over the network. In addition, determine whether connections you examine are encrypted-because you will not be able to read the contents of an encrypted session.

b) Analyse Host Data

Host data includes information about such components as the operating system and applications. The following procedure is used to analyse the copy of the host data obtained in the acquisition of the data phase.

- Identify what you are looking for. There will likely be a large amount of host data, and only a portion of that data might be relevant to the incident. Therefore, you should try to create search criteria for events of interest.
- Examine the operating system data, including clock drift information, and any data loaded into the host computer's memory to see if you can determine whether any malicious applications or processes are running or scheduled to run.
- Examine the running applications, processes, and network connections.

c) Analyse storage media

The following procedure is to be followed to extract and analyse data from the storage media collected:-

- Whenever possible, perform offline analysis on a bit-wise copy of the original evidence.
- Determine whether data encryption was used, such as the Encrypting File System (EFS) in Microsoft Windows. Several registry keys can be examined to determine whether EFS was ever used on the computer. If you suspect data encryption was used, then you need to determine whether or not you can actually recover and read the encrypted data.

- If necessary, uncompress any compressed files and archives. Although most forensic software can read compressed files from a disk image, you might need to uncompress archive files to examine all files on the media you are analysing.
- Create a diagram of the directory structure. It might be useful to graphically represent the structure of the directories and files on the storage media to effectively analyse the files.
- Identify files of interest.
- Examine the registry, the database that contains Windows configuration information, for information about the computer boot process, installed applications (including those loaded during startup), and login information such as username and logon domain.
- Study the metadata of files of interest, using tools such as Encase by Guidance Software, The Forensic Toolkit (FTK) by AccessData, or ProDiscover by Technology Pathways. File attributes such as timestamps can show the creation, last access, and last written times, which can often be helpful when investigating an incident.
- Use file viewers to view the content of the identified files, which allow you to scan and preview certain files without the original application that created them. This theapproach protects files from accidental damage and is often more cost-effective than using the native application. Note that file viewers are specific to each type of file; if a viewer is not available, use the native application to examine the file.[12]

- **REPORT THE INVESTIGATION**

There is a two-step process to organize the information that you gather and the documentation that you create throughout a computer investigation.

a) Gather and Organize information

The following procedure is to be followed to gather and organize the required documentation for the final report.

[12] Legal Aspects of Digital Forensics by Daniel J. Ryan and Gal Shpantzer

- Gather all documentation and notes from the Assess, Acquire, and Analyse phases. Include any appropriate background information.
- Identify parts of the documentation that are relevant to the investigation.
- Identify facts to support the conclusions you will make in the report.
- Create a list of all evidence to be submitted with the report.
- List any conclusions you wish to make in your report.
- Organize and classify the information you gather to ensure that a clear and concise report is the result.

b) Write a report

The following list identifies recommended report sections and information that should be included:-

- Purpose of report
- Author of report
- Incident summary
- Evidence
- Details i.e., description of what evidence was analysed and the analysis methods that were used.
- Conclusion
- Supporting documents

1.10 LET'S SUM UP

In this chapter, we have studied the evolution of computer forensics along with the basic concepts and objectives of computer forensics. We also studied the uses and ethics that need to be followed by the digital forensics expert. Finally, we ended our discussion with the Computer Forensics Investigation process.

1.11 FURTHER READING

- P. Y. S. B. D. C. A. U. Bansal, "Cyber Forensics-The art of Decoding the Binary Digits," International Journal of Emerging Technology and advanced engineering, vol. 2.
- Rogers MK, Seigfried K. The future of computer forensics: a needs analysis survey. Computers Security 2004 Feb;23(1): 12-16.
- MansonD,CarlinA,RamosS,GygerA,KaufmanM,TreicheltJ. Is the open way a better way? Digital Forensics using Open Source Tools. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
- Karyda M, Mitrou L. Internet forensics: legal and technical issues. Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 2007.
- Garfinkel SL. Automating Disk Forensic Processing with SleuthKit, XML and Python, 2009. Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Conference at Berkeley, California, USA.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the objectives of computer forensics?

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim's computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analysing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides a complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

2. What are the uses of computer forensics?

The uses of computer forensics include the following:

- Detecting a cybercrime.
- Solving an alleged criminal activity provided the medium used in perpetrating the crime is a digital device.
- Forestalling a crime from taking place.
- Computer forensics investigations are often used to refute or support a supposition during civil, criminal and corporate litigations.
- Computer forensics is used in the private sector by companies who are undergoing internal investigations into unauthorized technical and network transgressions.

3. What are the implications of digital forensics?

Digital forensics is commonly used in both criminal law and private investigation. Traditionally, it has been associated with criminal law, where the evidence is collected to support or oppose a hypothesis before the court of law. As with other areas of forensics, this is often a part of wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings. As a result, intelligence gathering is sometimes held to a less strict forensic standard. In civil litigation or corporate matters, digital forensics forms part of the electronic discovery process. Forensic procedures are similar to those in criminal investigations, often with different legal requirements and limitations. Outside of the courts, digital forensics can form a part of internal corporate investigations. The main focus of digital forensics investigations is to recover objective evidence of criminal activity (termed actusreus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

1.13 ACTIVITY

Explain the different phases of investigation process with the help of diagram? Explain it with an example. (1000-1500 words)

Unit 2: Overview of Digital Records and Cyber Forensics

2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction to Digital Records

1.3 Definition and scope

1.4 Characteristics and types

1.5 Advantages and Disadvantages

1.6 Relevance to E-commerce and E-governance

1.7 Introduction to Cyber forensics

1.8 Definition

1.9 Forensic Science

1.10 Elements of crime

1.11 Knowledge required for Cyber Forensic

1.12 Classification of Cyber Forensics

1.13 Key element of Cyber Forensics

1.14 How Cyber Forensics can help Investigating Officer

1.15 Let's sum up

1.16 Further reading

1.17 Check your progress: Possible answers

1.18 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Define digital records, its types and characteristics
- Forensic Science and Definition of Cyber Forensics
- Key Elements and Classification of Cyber Forensics

- Know how Cyber Forensics is used by investigating officer

1.2 INTRODUCTION TO DIGITAL RECORDS

In the current era of digitalisation, use of technology to transfer the paper-based information into digital information is very much common with every organisation. Technological advancement has made this change easier through different means. Digitalised information does not only give us the ease of access but also better storage in comparison with paper-based data. But digitalisation is not only limited to convert information from traditional way to technological way. Whatever new data is getting generated, gather and created is directly getting digitalised and it leads to new concepts like big data because the number of digital records is increasing tremendously day by day.[13]

The information residing in computing devices is in the form of 0's and 1's, this is also known as the mother tongue of computers (binary). All the information is nothing but the combination of digits (0's and 1's) hence we call them digital. Whatever the information is being stored in the digital format is been accessed with the help of software in human understandable form. Together this digital information is called as digital records. This digital information is mainly stored in different storage devices in different formats.

1.3 DEFINITION AND SCOPE

Digital record is the information which is mainly stored in computing devices in the form of 0's and 1's.

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

[13] The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010

Digital record is also defined as a record created or maintained by means of digital computer technology which includes records that are born digital or have undergone conversion from a non-digital format.[14]

It is a record which is maintained in a coded numeric format that can be accessed using a combination of hardware and software which translates them into text or images which can be comprehended by the human eye.

1.4 CHARACTERISTICS AND TYPES

The information in the form of digital records correctly reflects certain characteristics

- ***Confidentiality***

  Confidentiality refers to only the authorized person could have access to the information. It is also equivalent to the privacy of data. In simple language, confidentiality is the measures undertaken to prevent sensitive information from reaching to wrong people while making sure the right people can access it.

  Example: Data encryption, User ID-Passwords etc.[15]

- ***Availability***

  Availability simply means the information should be available in required format whenever needed. That means protecting the information from intentional as well as non-intentional loses. It is making sure that information is available for use all the time.

  Example: Performing hardware repairs, troubleshooting operating system issues, enough bandwidth availability preventing bottlenecks etc.

- ***Integrity***

  Integrity means maintaining the state of the information constant throughout its lifecycle. It also means consistency accuracy and trustworthiness of the data. The information should not change in transit also, it should be protected from alteration by unauthorized people.

- ***Authenticity***

[14] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016

[15] Forensic Examination of Digital Evidence: A Guide for Law Enforcement

The authenticity of the information mainly involves proof of identity. Which means it is the assurance that the information is from the source it claims to be from. Authentication is used to verify authenticity.

- ***Reliability***

  A reliable record is the one whose content is full, accurate and trustworthy. Reliable records are mainly used for interpretation and conclusion.

- ***Usability***

  It is the characteristic is recorded which mainly addresses further use of the digitally stored information. It is the record which should be located, retrieved and interpreted.

TYPES OF DIGITAL RECORDS

Based on the type of information, Digital records are classified as follows:

- ***Image File***

  This record mainly contains still images in the form of photographs. These images are stored in a variety of data formats such as JPEG (Joint Photographic Experts Group), TIFF (Tagged Image File Format), GIF (Graphic Interchange Format) etc.[16]

- ***Text File***

  This digital record mainly consists of different type of text which includes Tables, Databases, and Logs etc. These digital records also contain File format like .DOC, .PPT, .XLS, .PDF (Portable Document Format).

- ***Audio File***

  In this type of digital records,the sound is recorded which can be originally produced from analogue or digital formats. The audio files have several characteristics like Sampling Frequency, Bit-depth, Mono or Stereo. The examples of audio files are.WAV, MP3 etc.

- ***Video File***

  Video file is nothing but moving images recording which can be synced with audio. Pixel array, Frame rate per second, Aspect Ratio, Bit Rate, High Definition are important

[16]Arkfeld, M R (2002-2006), Electronic Discovery and Evidence. Law Partner Publishing, LLC. Phoenix, Arizona

characteristics of video files. The examples of video files are.AVI (Audio Video interleave), .MXF (Material Exchange Format), .WMV (Windows Media File) etc.

- ***Mark-up Language***

  This file format mainly contains embedded instruction for displaying the content over the website. This file is responsible for the text and graphical representation of the information over the World Wide Web. Examples of these files are.HTML (HyperText Mark-up Language), .XML (Extensible Mark-up Language) etc.

1.5 ADVANTAGES AND DISADVANTAGES

ADVANTAGES OF DIGITAL RECORDS

- **Easy to gather, store and access**

  Due to the different types of input available, it becomes very easy to collect and store information digitally. Example: Barcode reader, Document scanner, Touch screen etc.[17]

- **Speed**

  Because of high computing power an advanced networking devices, it's becoming faster to transmit, search and processing of the digital information.

- **Cost**

  Cost for overall digital records is comparatively cheaper in many aspects like storage, transmission etc.

- **Multimedia**

  This gives added advantage to represent the information in more presentable and active ways.

DISADVANTAGES OF DIGITAL RECORDS

- **Equipment Cost**

  When an organisation goes paperless there isa huge volume of data which is held on paper have to be converted to digital format. The cost of hardware and software needed

[17] Boucher, K, and Endicott-Popovsky, B (2008), "Digital Forensics and Records Management: What We can Learn from the Discipline of Archiving"

for this holds a substantial amount of money. This infrastructure also becomes obsolete in a relatively short time.

- **Privacy and security issue**

  As digital information increases, the functionality aspect like access and availability, privacy and security decreases reciprocally.

1.6 RELAVENCE TO E-COMMERCE AND E-GOVERNANCE

The digital India programme is a flagship program of the Government of India with a vision to transform India into digitally empowered society and knowledge economy. Information technology Act 2000 mainly addresses the legal recognition of digital records in e-commerce and e-governance.[18]

E-commerce is also known as electronic commerce is the activity of commercial transactions carried through computing and networking devices. E-commerce activity is rapidly growing in India which adds around 6 million new entrants every month. Amazon, Flipkart, Paytm, Snapdeal are few examples of E-commerce companies in India.

E-governance is defined as the use of computing technology and networking across government departments. It mainly involves the conversion of the paper base transaction into digital records. This has bought many projects under digitalisation namely Income Tax, Passport, Land records, Insurance, Visa immigration etc.

1.7 INTRODUCTION TO CYBER FORENSICS

Cyber Forensics is a rapidly growing field of forensics which mainly addresses all sort of digital evidence. Due to the increasing use of technology in everyday life, there are lots of digital records gets generated every now and then in different computing devices. These digital footprints come very handily during the investigation of all sort of criminal activities. Cyber

[18] Richard III GG, Roussev V Next-generation digital forensics Communications of the ACM. 2006 Feb 1;49(2):76-80

forensics gives us an in-depth view and understanding of these digital records in various situations. Hence, cyber forensics is not only used by the government but also private organisations.

1.8 DEFINITION

Cyber Forensics mainly consists of the integration of two terminologies as Cyber and Forensics. Cyber is defined as a space created by interconnected computer devices across the globe. The word cyber refers to digitalisation, the culture of computers and information technology.

Forensic means suitable for use in a court of law. Hence, Cyber forensics is defined as a branch of forensic science which addressed the recovery and investigation of the evidence found in digital devices. It is also sometimes referred to as digital forensics because of the direct relation with digital records.

Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

Cyber forensics is the application of investigation to search, gather and preserve the evidences from computing device in a way that is suitable for presentation in a court of law. CERT (Computer Emergency Response Team) defines cyber forensics as the process of using scientific knowledge for collecting analysing and presenting evidence to the court.

1.9 FORENSIC SCIENCE

Forensic science deals with recovery and analysis of latent evidence. Latent evidence may have different forms right from fingerprints on the glass to DNA evidence recovered from blood stains to the deleted SMS of mobile phones. The main objective of forensic science is to find out what has happened, who is affected, what has been used, how it has been used and who has committed the act. The first objective is to gather all the facts around this. Next objective is to present the data in a manner which is acceptable for the court. Forensic science is the application of science governed by legal standards of admissible evidence and criminal procedures. Forensic scientists are the group of people responsible to carry out the tasks of forensics namely collecting,

preserving and analysing scientific evidence during the course of the investigation. Many times forensic scientist visits the scene of the crime to collect the evidence in a proper forensic manner. Forensic scientist also gets testified as an expert witness in both criminal and civil cases.[19]

In the recent decade, documenting forensic science has become more efficient. Forensic scientists have started using advanced technologies in forensic processes. It has resulted in the accuracy of findings and also helped into logical reasoning of the incident. Unlike other areas of technology, forensic science has made significant growth and contributed to the court proceedings by eliminating all the doubts of prosecution towards the evidence.

1.10 ELEMENT OF CRIME

The legal definition of all crimes contains certain elements. If the government is not able to prove the existence of these elements then the conviction cannot be obtained in a court of law. That means crime can be broken down into elements which should be proved beyond a reasonable doubt by the prosecution. There are three main elements of every crime:

1. ***Criminal Act***

   It is the activity prohibited by law. It is also referred to as conduct which means an action carried out by accuse.

2. ***Criminal Intent***

   It is also called a purpose or state of mind resulted in a criminal act. It is further classified into four categories

- Purposely
- Knowingly
- Recklessly
- Negligently

3. ***Concurrence***

   Concurrence means the occurrence of both the above two elements at the same time.

Apart from these three, there are other elements of crime such as

[19]Carrier B Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence. 2003 Jan;1(4):1-2

- ***Law***

  There must be some law which addresses the act. That may sound obvious but there are certain acts which are objectionable but not criminal. Example Parking a vehicle in front of someone's gate.

- ***Burden of Proof***

  Depending on the case, the allegations or defence made in the court has to be proved beyond a reasonable doubt. The burden of the proof mainly lies with the one who makes certain statements in the court.

- ***Exculpatory Evidence***

  This is an important concept regarding the evidence that proves the accused innocence. In a criminal case, prosecutors have a legal duty to turnover exculpatory evidence to the defence.

1.11 KNOWLEDGE REQUIRED FOR CYBER FORENSICS

Cyber Forensics requires an understanding of various computing and networking concepts.[20] As cyber forensics consists of different technologies related to digital devices, the investigator should have solid background knowledge of the following topics:-

Hardware

On cannot perform forensic analysis without the knowledge of computer paths. That means the investigator should have a working knowledge of motherboard, Processor, Hard Drives, RAM and Expansion slots.

Hard Drives

Hard drives record and store the data in magnetic form on platters. The platters are organised on the spindle with Reading/Write head.

The data is organised as follows

- A sector is a basic unit of data storage on the hard disk which consists of 512 bytes.
- A cluster is a logical group of sectors.

[20]Breeuwsma, Marcel, et al "Forensic data recovery from flash memory." Small Scale Digital Device Forensics Journal 1.1 (2007): 1-17

- Sectors are in turn organised by tracks.

There are four types of hard drives:

1. SCSI- Small Computer System Interface
2. IDE- Integrated Drive Electronics
3. SATA- Serial Advanced Technology Attachment
4. SSD- Solid State Drive

RAM (Random Access Memory)

RAM plays a vital role ina forensic investigation point of view. Sometimes it's important to carry out forensics of running machine. For that, live memory capture is required. That means to take what is currently in RAM. Hence, live memory capture become quite important.

Following are the different types of RAM:

- DRAM (Dynamic RAM)
- SGRAM (Synchronous Graphic RAM)
- PSRAM (Pseudo-Static RAM)
- RLDRAM (Reduced Latency RAM)

Operating System

Operating systems are responsible for different operations on the machine. Cyber forensic approach changes with different operating systems. Hence, detailed knowledge of operating system enhances forensic investigation.[21]

Following are some of the examples of Operating System:

- Windows
- LINUX
- Macintosh
- IOS
- Android

Files and File Systems

The file system is the way through which computer organises data on a disk. Knowledge of file system gives added advantage to the investigator.

Following are some examples of file systems:

[21] SWGDE Best Practices for Computer Forensics, Scientific Working Group for Digital Evidence, Version 2.1

- FAT (File Allocation Table)
- NTFS (New Technology File System)
- EXT (Extended File System)

Networks

Many cybercrimes take place across the network. Strong understanding of the basics of networking helpsthe forensic investigator to unearth the important findings to different networking devices and related technologies. Hence, it is advised to have the following device and technologies:

Network topologies, Types of the network (LAN, WAN etc),Types of cables, WiFi, Hub, Switch, Router,Networking protocols etc.

1.12 CLASSIFICATION OF CYBER FORENSICS

Cyber forensics is an emerging practice to discover digital evidence through different computing devices and prosecute the criminals in a court of law. These digital footprints spread across multiple gadgets used by criminals. Cyber forensics is classified into many sub-branches depending upon the technology used for the storage of information in different computing devices around us.

Disk Forensics

It is also called as storage device forensics. It mainly deals with extracting information by searching the required data through active and deleted files. This field of forensics also targets unallocated and slack spaces of storage media.

Mobile Device Forensics

This branch mainly addresses forensics of all cellular devices like mobile, tablet, pagers etc. Mobile forensic retrieves the information like address book, call logs, SMS, photos, videos, audios etc.

Network Forensics

It mainly focuses on monitoring and analysing network traffic for the purpose of intrusion detection, information gathering, legal evidence etc. It is one of the proactive forensic investigation techniques. It also includes a log analysis of different networking devices.

Database Forensics

In many software, information is stored in the form of a database. Hence, database forensics comes very handy in order to retrieve information related to databases. It mainly consists of metadata analysis, timestamp analysis and deleted record recovery of the databases.

Malware Forensics

It mainly deals with investigating and analysing malicious code in the system which may be in the form of Virus, Worm, Trojan, and Rootkit etc.

Email Forensics

This branch of forensics is responsible for recovery and analysis of emails which includes email source investigations, email attachments, contacts and calendar invites of email etc.

Memory Forensics

It aims at collecting and analysing information from system memory in the raw form. The system memory mainly consists of system register, cache and RAM.

Wireless Forensics

It is a subcategory of Network Forensics which targets the methodology and tools required to collect and analyse wireless network traffic data.

1.13 KEY ELEMENTS OF CYBER FORENSICS

Following are the key elements which encompass cyber forensics:

The Identification and Acquisition of Digital Evidence

It is important to have knowledge of possible evidences lying around the crime scene. The cyber forensic investigator should be able to identify the type of information stored in a device and also the format of that data. With the help of this information, the appropriate technology can be decided to extract the evidence. The acquisition process can vary device to device. During the acquisition process, the investigator can acquire the evidence either by creating an image or by cloning the disk.

Preservation of Digital Evidence

This is a critical element of forensic investigation in which the evidence is stored by protecting it against any type of alteration or tampering.

The Analysis of Digital Evidence

This element consists of loading, processing, extracting of the identified evidence. This is the main element of cyber forensics. The extraction produces a binary data which should be analysed and processed to convert it into human-readable form.

The Reporting of Digital Evidence

This element consists of a collection of all the findings stated in such a way that it can be understood by any person. The report should be in very simple terms giving the description of the item mainly findings and conclusion.

Presentation of the Digital Evidence

This element is directly related to the representation to the court of law. The proper representation increases the chances of admissibility of the evidence.

1.14 HOW CYBER FORENSICS HELP INVESTIGATING OFFICER

Discover all files

A casual viewer may not able to view all the files present over the system. Through forensic view, investigator can discover all the files which are present on the system which includes hidden files, password-protected files, encrypted files, hidden files etc.

Data Recovery

Cyber forensics helps into the recovery of the deleted files from the disc. Cyber forensics can also carve overwritten files to extract data to some extent. Data recovery also unearths the files from unallocated or slacks space of the discs.

Keyword Search

Cyber forensics helps to index of the hug information which ultimately helps investigator to find out the relevant evidences effectively and faster.

Timeline Analysis

Cyber forensics can give the proper timeline of the identified evidence with the help of different metadata and event logs of the system. With the help of timeline analysis, the investigator can have detailed knowledge of when particular evidence been created, accessed and used for the crime.

Volatile Evidence Analysis

Forensics of volatile data helps the investigator to know what is currently happening on the system. It can be done by the analysis of RAM and cache memory. This also gives added advantage to monitor live attacks.

Root Cause Analysis (RAC)

Cyber Forensics can help the investigator to identify the root cause of the said crime by complete analysis of the computing devices involved in a particular act.

Despite all above cyber forensics can also be used for some other reasons like

Operational Troubleshooting

Better incidence response and recovery

Log Monitoring

Data Preservation

Business Continuity

Better Vulnerability Detection

1.15 LET'S SUM UP

In this chapter, we have studied the concept of digital records and cyber forensics along with its characteristics, advantages and disadvantages and types. We also studied how it is relevant to e-commerce and e-governance. Finally, we ended our discussion with how cyber forensics can help the investigating officers.

1.16 FURTHER READING

- Nina Godbole and SunitBelapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
- Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.

1.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are digital records?**

Digital record is a form of electronic record which is electronically generated or stored in different storage devices.

2. **What are the different types of digital records?**

Digital records are classified as follows:

- Image File
- Text File
- Audio File
- Video File
- Mark-up Language

3. **What is cyber forensics?**

   Cyber forensics is a branch of forensic science which aims at a constructive way of identifying, reserving analysing, recovering and presenting the digital evidence in a court of law.

4. **What are the different types of cyber forensics?**

Cyber forensics is classified into many sub-branches depending upon the technology used for storage of information in different computing devices around us.

- Disk Forensics
- Mobile Device Forensics
- Network Forensics
- Database Forensics
- Malware Forensics
- Email Forensics
- Memory Forensics
- Wireless Forensics

1.18 ACTIVITY

Briefly explain the meaning of cyber forensics along with its elements that are used in crime scene and its classification? Also, elucidate in what way cyber forensics can help the investigating offices with a case study. (1500 words)

Unit 3: Investigation Process

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 ACPO Guidelines

1.4 Digital Evidence Guidelines

1.5 Steps in Crime Scene Investigation

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The process of investigation
- Different guidelines for digital evidence
- Understand step wise instruction of investigation in different scenarios

1.2 INTRODUCTION

Nowadays investigation is been carried out at a very fast pace. Thanks to technology that help investigating officer to gather the relevant information at very high speed and act upon it. Investigation process used needs to update and enhance with net types of technological advancement. In this chapter, we will understand the different investigation processes, guidelines

and standard operating procedure which investigation officer needs to be followed while dealing with cyber-crimes and other crimes where digital evidence are involved.[22]

1.3 ACPO GUIDELINES

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-based Electronic Evidence [ACPO] –for reference

- No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.
- Individuals accessing original data must be competent to do so and have the ability to explain their actions.
- A trail or other record of applied processes, suitable for replication of the results by an independent third-party, must be created and preserved, accurately documenting each investigative step.
- The person in charge of the investigation has overall responsibility for ensuring the above-mentioned procedures are followed and in compliance with governing laws.

Apart from ACPO guidelines there are several guidelines out there and mainly used by Indian law enforcement agencies as given below.[23]

1.4 DIGITAL EVIDENCE GUIDELINES

- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any

[22] See the Digital Records Forensics Project website at <http://digitalrecordsforensics.org>

[23] Adams, Richard & Hobbs, Val & Mann, Graham.(2014). Journal of Digital Forensics, Security & Law.Journal of Digital Forensics, Security & Law. 8. 25-48

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized[24]

Following is the simple diagram which represents how exactly the cybercrime investigation is been carried out.[25]

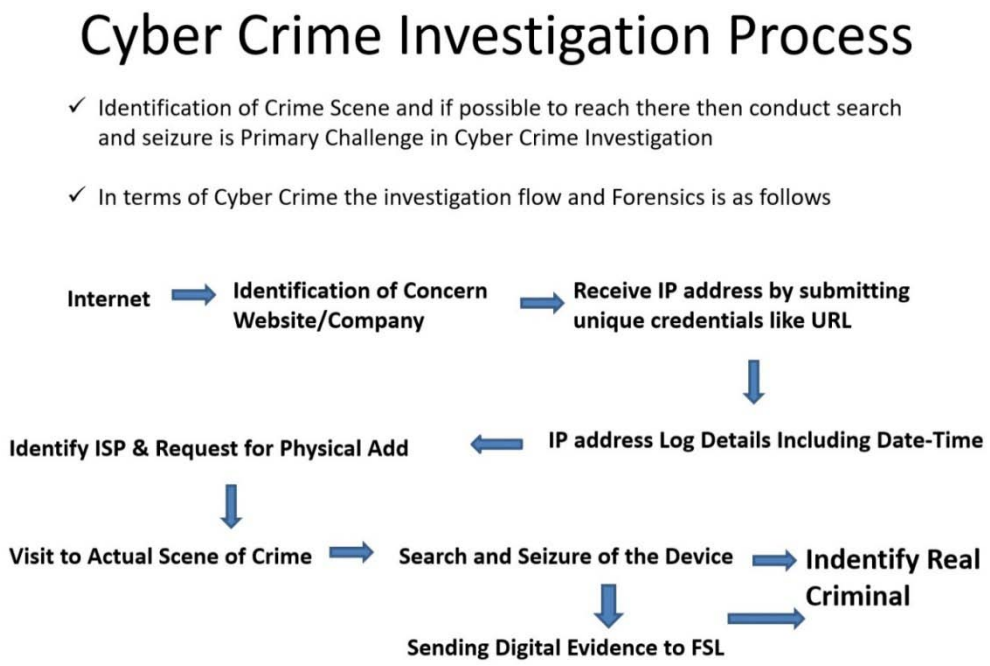


Figure 1.1 Cyber Crime Investigation Process

In the above diagram, the cyber space-related investigation is described. It mainly explains the flow of investigation where the place of incident is the internet.

Now let's understand the step by step approach of the investigating officer in crime investigation.

[24] Adams, R (2013) Doctoral Thesis. The Advanced Data Acquisition Model (ADAM): A process model fordigital forensic practice Murdoch University Retrieved from <http://researchrepository.murdoch.edu.au/14422/2/02Whole.pdf>

[25] Agarwal, A, Gupta, M, Gupta, S, & Gupta, S C (2011).Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118-130

1.5 STEPS IN CRIME SCENE INVESTIGATION

1. Identifying and securing the crime scene[26]
2. 'As is where is' documentation of the scene of the offence
3. Collection of evidence
4. Procedure for gathering evidences from switched-off Systems
5. Procedure for gathering evidence from live systems
6. Forensic duplication
7. Conducting interviews
8. Labelling and, documenting the evidence
9. Packaging, and transportation of the evidences

THE PROCESS OF EVALUATION OF THE SCENE OF OFFENCE

- Secure the Scene of Crime
- Identify all the potential evidences
- Conventional evidences like sticky slips, manuals, bank account numbers etc., to be part of the search process.
- If the system is OFF, leave it OFF
- Special care to be taken for perishable evidence eg., volatile data
- After identifying the scene of the offence, IO should secure it and, take note of every individual physically present at the scene of offence and, their role at the time of securing the scene of offence.
- From the information gathered and based on visual inspection of the scene of offence, IO should identify all the potential evidence. These physical evidences may include conventional physical evidences like the manuals, user guides and, other items left behind like passwords on slips, bank account numbers etc. it is also important to note the position of the various equipment and items at the scene of offence. For example,

[26]Ciardhuain, S O (2004)An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(1)

a mouse on the left-hand side of the desktop possibly indicates the person operating the computer is a left-handed user.[27]

- While identifying the digital evidence, IO should make sure that the potentially perishable evidence is identified and, all the precautions are put in place for its preservation.

FOLLOWING IS THE PROCEDURE FOR CONDUCTING SEARCH

1. Secure the spot
2. Preserve the fingerprints
3. Restrict the access to a computer (s)
4. Don't accept the help of the suspect for operating computer.
5. Make the Computers Standalone (Remove LAN / Telephone / Wi-Fi / Blue tooth etc)
6. If the computer is/are "OFF"; don't turn "ON"
7. Some screen savers will show that computer is off hence to make sure by checking the light of CPU.
8. If the computer is "ON" then note down the date and time of computer system, don't try to correct it.
9. Documentation
10. Take the photograph of the Monitor screen
11. Don't shutdown the computer in a normal manner but for shutting down pull the power cord from CPU and not from wall point.
12. Place the unformatted blank floppies in each drive for preventing accidental booting of the computer.
13. Photograph the scene, then disconnect all power source; unplug from wall and also from the back of the system.
14. Draw the sketch of the scene of the spot.
15. Label all the equipment, connectors and cables ends to allow reassemble as needed.
16. Seal all the ports and also screws of the CPU with paper seal.

[27]Freiling, F C, &Schwittay, B (2007) A common process model for incident response and computer forensics. Paper presented at the Conference on IT Incident Management and IT Forensics, Germany

17. Pack and seal the equipment carefully and a sample of the same seal must be sent to the FSL where the analysis of the CPU will be carried out.
18. Examine the persons, including suspect for the passwords, username etc.
19. Search the premises for the printouts, handwritten notes, diary, notebooks etc., for the passwords, username etc.
20. Search the premises for the software/programs, printouts, handwritten notes, financial transactions, books etc., which may be of vital importance to the investigation.
21. In personal search look for the pen/flash drives which might be attached to a key chain and may contain vital data.

PRELIMINARY INTERVIEWS AT THE SCENE OF OFFENCE

Following are some of the key questions which should be discussed during this phase of the investigation.[28]

- What steps were taken to contain the issue?
- Were there any logs (system access, etc.) present that cover the issue?
- Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred.
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained?
- Are there any questions about the issue that have not been answered?

AT THE SCENE OF OFFENCE, IO SHOULD GATHER THE FOLLOWING INFORMATION DURING THE INTERVIEWS PHASE

[28] Palmer, G (2001) A Road Map for Digital Forensic Research. Digital Forensics Research Workshop, Utica, New York

- Identify the complainant/owner (s) of the various devices and obtain the access details, usernames, and service providers' details.
- Gather information as provided in the questionnaire(s) above, on all the security systems
- Identify the list of the people who can identify the network and a schematic diagram of the network

Let's take some examples in order to understand the investigation process of the different scene of the crime.[29]

SCENE OF OFFENCE: CYBER CAFÉ

1. Identify the number of computer systems present in the cyber café.
2. Identify the number of computer systems connected to the Internet.
3. Obtain details about the network topology and architecture (client — Server).
4. Obtain the CCTV/Web camera clippings, if any.
5. Whether any user management software is used by the cyber café owner?
6. Obtain the log register of Internet users for the relevant period.
7. Check the formatting of storage devices policy adopted by the cyber café owner.
8. Check the hardware replacements done by the cyber café owner.
9. Check the policy regarding removal media usage on the cyber café systems.

SCENE OF OFFENCE: HOME

1. Identify the type of connection (Wi-Fi/Ethernet).
2. How many computer systems are used for the Internet connection?
3. Location of the system and details of persons with access to system(s).
4. Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
5. Obtain details about the network topology and architecture (client — Server), if any.
6. Obtain the details about other computer peripherals (printer/scanner/modem, etc.).

ISSUANCE OF THE PRESERVATION NOTICE

[29]Selamat, S R, Yusof, R, & Sahib, S (2008) Mapping process of digital forensic investigation framework. International Journal of Computer Science and Network Security, 8(10)

Preservation notice is the formal and legal document made in order to request to preserve the information which is important for further investigation. This is the vital document in the investigation process of the digital evidence.

Based on the information gathered, the IO should come out with issues to be complied immediately by issuing specific do's and don'ts to the complainant/company/agency.

e.g. stopping the access, taking backups, or preserving log information, etc. till further orders. For example, continuing access to the e-mail by the accused can enable him to delete the mails which are incriminating in nature.

A preservation notice needs to be sent to all affected parties to make sure that they do not delete any data that could be relevant to the case. It is ideal to issue this notice, which is necessary for preserving evidence.

GATHERING EVIDENCE

In this phase it is important to know the standard operating procedures for gathering information from different pieces of evidence. SOP gives step by step approach to gather evidence in a legal manner and preserve its admissibility by protecting the integrity of the evidence

PROCEDURE FOR GATHERING EVIDENCES FROM SWITCHED-OFF SYSTEMS

- Secure and take control of the scene of crime both physically and electronically.
- Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON.
- Be aware that some laptop computers may power ON by opening the lid.
- Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the system.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary

- Carefully open the side casing of the CPU or laptop and identify the Hard disk. Detach the hard disk from the motherboard by disconnecting the data transfer cable and power cable.
- Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number.
- Get the signature of the accused and witness on Hard disk, by using a permanent marker. Ensure that all items have signed and completed exhibit labels.
- Search scene of the crime for Non-electronic evidences like diaries, notebooks or pieces of paper with passwords.

PROCEDURE FOR GATHERING EVIDENCES FROM LIVE SYSTEMS (SWITCHED-ON SYSTEMS)

- Record what is on the screen by a photograph and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph/video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.
- Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

PROCEDURE FOR GATHERING EVIDENCES FROM MOBILE PHONES

- If the device is “OFF”, do not turn “ON”.
- With PDAs or cell phones, if the device is ON, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).

- Label and collect all cables (including power supply) and transport with device.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in the seizure of device and components.

USE OF FARADAY BAD IN MOBILE SEIZURE

Benefits for the investigator if a faraday bag is used are:

1) Potentially avoids the problem of the mobile phone becoming PIN locked.
2) Faraday Window ensures the examiner to view the phone in a 'faraday' condition, thus enabling an 'immediate preview of evidence'.
3) Re-usable
4) To prevent the data from the networks communicating with the device, therefore, stops any chance of evidence being tainted.
5) Prevents any chance of evidence being manipulated during covert acquisition.

After gathering the evidence it needs to be sent to Forensic lab for the analysis and reporting of it. With the evidence, the investigation officer needs to send certain points which act as guidelines for the forensic expert to retrieve the evidence from the sent media. Hence to get the best of the expert opinion IO should follow the following process.[30]

EXPERT OPINION FROM FORENSIC EXAMINER

- The forwarding letter to the FSL for scientific analysis and opinion should mention the following information.
- A brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of the crime
- The condition of the computer system (on or off) at the scene of the crime
- Is the photograph of the scene of crime is taken?

[30]Venter, J P (2006). Process flows for cyber forensics training and operations Retrieved from <http:researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter_2006.pdf>

- Is it a stand-alone computer or a network?
- Is the computer has an Internet connection or any means to communicate with external computers?

MODEL QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS A TARGET" CYBERCRIME

- What type of operating system has been installed on the computer?
- When was the operating system installed?
- Please provide the user names/users present in the system
- What programs or software is installed on the computer?
- What is the IP address assigned to the system, if any?
- What is the MAC address of the system?
- Are there any information relating e-mail addresses present in the computer system?
- Are there any chat messenger software installed. If so, are there any chat IDs/profiles?
- Any suspicious or malicious software installed?
- Please provide the Internet history of the computer (Web sites accessed, files uploaded, downloaded, etc.)?
- Are there any firewall logs available in the system?

QUESTIONS TO BE ASKED IN CASE OF "SENDING THREATENING E-MAIL"

- Whether the sender's e-mail address is present in the seized hard disk.
- Whether the receiver's e-mail address is present in the seized hard disk.
- Whether the contents of the e-mail message (subject mail of case) is present in the hard disk.
- Any information relating to the IP addresses are available?

QUESTIONS TO BE ASKED IN CASE OF "COMPUTER AS AN INSTRUMENT/REPOSITORY"

- Which are the user accounts that are present on the computer?
- What financial applications/software applications are installed in the system?
- Are there any logs available for these applications?
- Please provide the list of files/filenames that were recently accessed
- What external devices (like thumb drives/external hard drives) were connected to the computer?

- Are there any databases and excel spreadsheets available inactive or deleted state?
- Are there any accounting packages/software installed?
- Are there any encrypted or password-protected files available? If so, please extract the content from them?
- Are there any pornographic images/videos present in the computer system?
- Was the system date and time changed at any point in time?

1.6 LET'S SUM UP

In this chapter, we have studied about the investigation process along with the ACPO guidelines. We also studied about the different guidelines with respect to digital evidence. Finally, we ended our discussion with the steps in crime scene investigation.

1.7 FURTHER READING

- Shon Harris; "All in One CISSP Guide, Exam Guide Sixth Edition", McGraw Hill, 2013.
- LNJN National Institute of Criminology and Forensic Science, "A Forensic Guide for Crime Investigators – Standard Operating Procedures", LNJN NICFS, 2016.
- Anthony Reyes, Jack Wiles; "The Best Damn Cybercrime and Digital Forensic Book", Syngress, USA, 2007.
- Cory Altheide and HalanCarvey; "Digital Forensics with Open Source Tools", Syngress Publication.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is ACPO?

The Association of Chief Police Officers (ACPO) was a not-for-profit private limited company that for many years led the development of policing practices in England, Wales, and Northern Ireland. It has contributed a lot in terms of guidelines for handling digital evidence.

2. What are the guidelines for digital evidence?

- Identify the computer system, Secure the scene, preserve the traced evidence
- If the computer is switched off, then Photograph, label and document the system.details on collection form and collect related software peripherals, removable media, passwords if any.

- If the computer is on and prompts for any password simply disconnect the power and then Photograph, label and document the system details on collection form and collect related software peripherals, removable media, passwords if any.
- If it does not prompts for any password, then document screen, system time, network activity. Preserve the RAM content if needed using Authorized tools and procedures.
- Depending upon the case Scenario, the entire computer can be seized or any particular suspected hardware can be seized.

3. Explain the scene of offence in cyber café?

- Identify a number of computer systems present in the cyber café.
- Identify a number of computer systems connected to the Internet.
- Obtain details about the network topology and architecture (client — Server).
- Obtain the CCTV/Web camera clippings, if any.
- Whether any user management software is used by the cyber café owner?
- Obtain the log register of Internet users for the relevant period.
- Check the formatting of storage devices policy adopted by the cyber café owner.
- Check the hardware replacements done by the cyber café owner.
- Check the policy regarding removal media usage on the cyber café systems.

1.9 ACTIVITY

Briefly explain the steps in a Crime Scene Investigation along with a case study? (1000 – 1500 words)

Unit 4: Electronics Discovery: An Introduction

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Legal basis of Electronic discovery

1.4 ESI Preservation: Obligations and Penalties

1.5 Determining violations of the Electronic discovery paradi

1.6 Assessing what data is reasonably accessible

1.7 Utilizing criminal procedure to accentuate E-discovery

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Legal basis of electronic discovery
- ESI preservations: Obligations and Penalties
- Utilizing criminal procedure to accentuate E-discovery

1.2 INTRODUCTION

Electronic discovery or "e-discovery" is the exchange of data between parties in civil or criminal litigation. The process is largely controlled by attorneys who determine what data should be produced based on relevance or withheld based on claims of privilege. Forensic examiners, however, play crucial roles as technical advisors, hands-on collectors, and analysts.

Some examiners view electronic discovery as a second-class endeavour, void of the investigative excitement of a trade secret case, an employment dispute, or a criminal "whodunit." These examiners, however, overlook the enormous opportunities and challenges presented by electronic discovery.[31]

In technical terms,electronic discovery also poses a variety of daunting questions: Where are all the potentially relevant data stored? What should a company do to recover data from antiquated, legacy systems or to extract data from more modern systems like enterprise portals and cloud storage? Does old data need to be converted? If so, will the conversion process result in errors or changes to important metadata? Is deleted information relevant to the case? What types of false positives are being generated by keyword hits? Did the tools used to process relevant data cause any errors or omissions in the information produced to lawyers? What file server data can be attributed to specific custodians? How can an examiner authenticate database reports? What can an examiner do to fill in the gaps after the e-mail has been erroneously deleted?

Confusion over terminology between lawyers, forensic examiners, and laypeople add to the complexity of e-discovery. For instance, a forensic examiner may use the term "image" to describe a forensic duplicate of a hard drive, whereas an IT manager may call routine backups an "image" of the system, and a lawyer may refer to a graphical rendering of a document (e.g., in TIFF format) as an "image." These differing interpretations can lead to misunderstandings and major problems in the e-discovery process, adding frustration to an already pressured situation.George Socha and Thomas Gelbman have created a widely accepted framework for e-discovery consulting known as the Electronic Discovery Reference Model (EDRM).The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;
b) Associate document collections with particular users (custodians);
c) Capture and preserve the metadata associated with the electronic files within the collections;
d) Establish the parent-child relationship between the various source data files;

[31]Stander, Adrie& Val, Kevin & Hooper, Val (2015).Ediscovery in South Africa and the Challenges it Faces

e) Automate the identification and elimination of redundant,duplicate data within the given dataset;
f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;
g) Unprotect and reveal information within files; and
h) Accomplish all of these goals in a manner that is both defensible with respect to clients' legal obligations and appropriately cost-effective and expedient in the context of the matter.[32]

1.3 LEGAL BASIS FOR ELECTRONIC DISCOVERY

In civil litigation throughout the United States, courts are governed by their respective rules of civil procedure. Each jurisdiction has its own set of rules, but the rules of different courts are very similar as a whole.1 As part of any piece of civil litigation, the parties engage in a process called discovery. In general, discovery allows each party to request and acquire relevant, nonprivilegedinformation in possession of the other parties to the litigation, as well as third parties (F.R.C.P. 26(b)). When that discoverable information is found in some sort of electronic or digital format (i.e., hard disk drive, compact disc, etc.), the process is called electronic discovery or e-discovery for short.

The right to discover ESI is now well established. On December 1, 2006, amended F.R.C.P. went into effect and directly addressed the discovery of ESI. Although states have not directly adopted the principles of these amendments en masse, many states have changed their rules to follow the 2006 F.R.C.P. amendments.

In ***Coleman vs Morgan Stanley***[33]**,** after submitting a certificate to the court stating that all relevant e-mail had been produced, Morgan Stanley found relevant e-mail on 1600 additional backup tapes. The judge decided not to admit the new e-mail messages, and based on the company's failure to comply with e-discovery requirements, the judge issued an "adverse inference" to the jury, namely that they could assume MorganStanley had engaged in fraud in the underlying investment case. As a result, Morgan Stanley was ordered to pay $1.5 billion in

[32]Arkfeld, M R (2005), Electronic Discovery and Evidence, Law Partner Publishing, LLC, Phoenix, AZ
[33]*Coleman v Morgan Stanley*20 So 3d 952 (Fla Dist Ct App) [2009]

compensatory and punitive damages. An appeals court later overturned this award, but the e-discovery findings were left standing, and the company still suffered embarrassing press like The Wall Street Journal article, "How Morgan Stanley botched a big case by fumbling e-mails" (Craig, 2005).

1.4 ESI PRESERVATION: OBLIGATIONS AND PENALTIES

Recent amendments to various rules of civil procedure require attorneys—and therefore digital examiners—to work much earlier, harder, and faster to identify and preserve potential evidence in a lawsuit. Unlike paper documents that can sit undisturbed in a filing cabinet for several years before being collected for litigation, many types of ESI are more fleeting. Drafts of smoking-gun memos can be intentionally or unwittingly deleted or overwritten by individual users, server-based e-mail can disappear automatically following a systematic purge of data in a mailbox that has grown too large, and archived e-mail can disappear from backup tapes that are being overwritten pursuant to a scheduled monthly tape rotation.[34]

The seminal case of ***Zubulake v. UBS Warburg***[35] outlined many ESI preservation duties in its decision. Laura Zubulake was hired as a senior salesperson to UBS Warburg. She eventually brought a lawsuit against the company for gender discrimination, and she requested, "all documents concerning any communication by or between UBS employees concerning Plaintiff." UBS produced about 100 e-mails and claimed that its production was complete, but Ms.Zubulake's counsel learned that UBS had not searched its backup tapes. What began as a fairly mundane employment action turned into a grand e-discovery battle, generating seven different opinions from the bench and resulting in one of the largest jury awards to a single employee in history.[36]

The court stated that "a party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant

[34] Carrier, B. 'Open Source Digital Forensics Tools: The Legal Argument', @stake Research Report, October 2002

35 *Zubulake v UBS Warburg*217 F R D 309 (S D N Y) [2003]

[36] Federal rules of evidence. Available online at <www.law.cornell.edu/rules/fre/rules.htm>

documents created thereafter," and outlined three groups of interested parties who should maintain ESI:

- **Primary players:** Those who are "likely to have discoverable information that the disclosing party may use to support its claims or defenses" (F.R.C.P. 26(a)(1)(A)).
- **Assistants to primary players:** Those who prepared documents for those individuals that can be readily identified.
- **Witnesses:**The duty also extends to information that is relevant to the claims or defenses of any party, or which is 'relevant to the subject matter involved in the action'" (F.R.C.P. 26(b)(1)).

The Zubulake court realized the particular difficulties associated with retrieving data from backup tapes and noted that they generally do not need to be saved or searched, but the court noted:

"It does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes".[37]

In addition to clarifying the preservation obligations in e-discovery, the Zubulake case revealed some of the penalties that can befall those who fail to meet these obligations.The court sanctioned UBS Warburg for failing to preserve and produce e-mail backup tapes and important messages, or for producing some evidence late. The court required the company to pay for additional depositions that explored how data had gone missing in the first place. The jury heard testimony about the missing evidence and returned a verdict for $29.3 million, including $20.2 million in punitive damages.

The Zubulake court held the attorneys partially responsible for the lost e-mail in the case and noted, "It is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." (Zubulake v. UBS Warburg, 2004). Increasingly, attorneys have taken this charge to heart and

[37] Magic Quadrant for E-Discovery Software, Gartner, 2014

frequently turn to their digital examiners to help assure that their discovery obligations are being met.

1.5 DETERMINING VIOLATIONS OF THE ELECTRONIC DISCOVERY PARADI

As pointed out by the Zubulake decision, the consequences of failing to preserve data early in a case can be severe. Under F.R.C.P. Rule 37, a court has broad latitude to sanction a party in a variety of ways. Of course, courts aremost concerned about attorneys or litigation parties that intentionally misrepresent the evidence in their possession, as seen in the Qualcomm case.[38]

The following 10 recommendations are provided for investigators and in-house counsel to avoid the same fate as Qualcomm (Roberts, 2008):

a) Use checklists and develop a standard discovery protocol;
b) Understand how and where your client maintains paper files and electronic information, as well as your client's business structures and practices;
c) Go to the location where information is maintained—do not rely entirely on the client to provide responsive materials to you;
d) Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;
e) Ask all witnesses about other potential witnesses and where and how evidence was maintained;
f) Use the right search terms to discover electronic information;
g) Bring your own IT staff to the client's location and have them work with the client's IT staff, employ e-discovery vendors or both;
h) Consider entering into an agreement with opposing counsel to stipulate the locations to be searched, the individuals whose computers and hard copy records are at issue, and the search terms to be used;
i) Err on the side of production;
j) Document all steps are taken to comply with your discovery protocol.

[38] Computer Technology Review, Sharon Isaacson, March 2003

This is a useful and thorough set of guidelines for investigators to use for preservation of data issues, and can also serve as a quick factsheet in preparing for depositions or testimony.

1.6 ASSESSING WHAT DATA IS REASONABLY ACCESSIBLE

Electronic discovery involves more than the identification and collection of data because attorneys must also decide whether the data meets three criteria for production. Namely, whether the information is (1) relevant, (2) nonprivileged, and (3) reasonably accessible (F.R.C.P. 26(b)(2)(B)). The first two criteria make sense intuitively. Nonrelevant information is not allowed at trial because it simply bogs downs the proceedings, and withholding privileged information makes sense in order to protect communications within special relationships in our society, for example, between attorneys and clients, doctors and patients, and such. Whether information is "reasonably accessible" is harder to determine, yet this is an important threshold question in any case.[39]

In the Zubulake case described earlier, the employee asked for "all documents concerning any communications by or between UBS employees concerning Plaintiff," which included "without limitation, electronic or computerized data compilations," to which UBS argued the request was overly broad. In that case, Judge Shira A. Scheindlin, United States District Court, Southern District of New York, identified three categories of reasonably accessible data: (1) active, online data such as hard drive information, (2) near-line data to include robotic tape libraries, and (3) offline storage such CDs or DVDs. The judge also identified two categories of data generally not considered to be reasonably accessible: (1) backup tapes and (2) erased, fragmented, and damaged data. Although there remains some debate about the reasonable accessibility of backup tapes used for archival purposes versus disaster recovery, many of Judge Scheindlin's distinctions were repeated in a 2005 Congressional report from the Honorable Lee H. Rosenthal,

[39]Ward, Burke and Sipior, Janice and Hopkins, Jamie and Purwin, Carolyn and Volonino, Linda, Electronic Discovery: Rules for a Digital Age (February 27, 2011) Boston University Journal of Science and Technology Law, Vol. 18, No. 150, 2012

Chair of the Advisory Committee on the Federal Rules of Civil Procedure (Rosenthal, 2005), and Zubulake's categories of information remain important guideposts (Mazza, 2007).[40]

The courts use two general factors—burden and cost—to determine the accessibility of different types of data. Using these general factors allows the courts to take into account the challenges of new technologies and any disparity in resources among parties (Moore, 2005). If ESI is not readily accessible due to burden or cost, then the party possessing that ESI may not have to produce it (see F.R.C.P. 26(b)). Some parties, however, make the mistake of assessing the burden and cost on their own and unilaterally decide not to preserve or disclose data that is hard to reach or costly to produce. The rules require that a party provide"a description by category and locations, of all documents" with potentially relevant data, both reasonably and not reasonably accessible (F.R.C.P. 26(a)(1)(B)). This allows the opposing side a chance to make a good cause showing to the court why that information should be produced (F.R.C.P. 26(a)(2)(B)).

1.7 UTILIZING CRIMINAL PROCEDURE TO ACCENTUATE E-DISCOVERY

In some cases, such as lawsuits involving fraud allegations or theft of trade secrets, digital examiners may find that the normal e-discovery process has been altered by the existence of a parallel criminal investigation. In those cases, digital examiners may be required to work with the office of a local US Attorney, State Attorney General, or District Attorney, since only these types of public officials, and not private citizens, can bring criminal suits.[41]

A criminal agency can preserve data early in an investigation by issuing a letter under 18 U.S.C. 2703(f) to a person or an entity like an Internet Service Provider (ISP). Based on the statute granting this authority, the notices are often called "f letters" for short. The letter does not force someone toproduce evidence but does require they preserve the information for 90 days (with the chance of an additional 90-day extension). This puts the party with potential evidence on notice

[40]Friedberg, E, & McGowan, M (2003).Electronic discovery technology. In A Cohen & D. Lender (Eds.), Electronic discovery: Law and practice, Aspen Publishers

[41] See Jonathan M Redgrave & Kristin M. Nimsger, Electronic Discovery and Inadvertent Productions of Privileged Document, THE FED. LAWYER, July 2002, at 37, available at <http://www.jonesday.com/files/>

and buys the agency some time to access that information or negotiate with the party to surrender it.[42]

Another less popular method of obtaining evidence is through a court "d" order, under 18 U.S.C. §2703(d). This rule is not used as often because an official must be able to state with "specific and articulately" facts that there is a reasonable belief that the targeted information is pertinent to the case. However, this method is still helpful to obtain more than just subscriber information—data such as Internet transactional information or a copy of a suspect's private homepage.

There are five digital storage locations that are the typical focus of e-discovery projects (Friedberg & McGowan, 2006):

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB "thumb" drives
- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

Although these storage locations are the typical focus of e-discovery projects, especially those where the data are being collected in a corporate environment, examiners should be aware of other types of storage locations that may be relevant such as digital media players and data stored by third parties (for example,Google Docs, Xdrive, Microsoft SkyDrive, blogs, and social networking sites such as MySpace and Facebook).

Informational interviews and documentation requests are the core components of a comprehensive and thorough investigation to identify the potentially relevant ESI in these five locations, followed by review and analysis of the information obtained to identify inconsistencies and gaps in the data collected. In some instances a physical search of the company premises and off-site storage is also necessary.

1.8 LET'S SUM UP

[42]Kidwell, B, Neumeier, M, & Hansen, B (2005) Electronic discovery. Law Journal Press

The e-discovery field is complex, and the technical and logistical challenges routinely found in large e-discovery projects can test even the most experienced digital forensic examiner. The high stakes nature of most e-discovery projects leave little room for error at any stage of the process—from initial identification and preservation of evidence sources to the final production and presentation of results—and to be successful, an examiner must understand and be familiar with their role at each stage. The size and scope of e-discovery projects require effective case management, and essential to effective case management is establishing a strategic plan at the outset, and diligently implementing constructive and documented quality assurance measures throughout each step of the process.

1.9 FURTHER READING

- ACPO. (2008). The Good Practice Guide for Computer-based Electronic evidence. (4th ed.). Available online at www.7safe.com/electronic_evidence/
- Craig, S. (2005). How Morgan Stanley botched a big case by fumbling emails. The Wall Street Journal, A1.
- Mazza, M., Quesada, E., & Sternberg, A. (2007). In pursuit of FRCP1: Creative approaches to cutting and shifting the costs of discovery of electronically stored information, 13 Rich. J.L. & Tech., 11, 101.
- Howell, B. (2009). Lawyers on the Hook: Counsel's professional responsibility to provide quality assurance in electronic discovery. Journal of Securities Law, Regulation & Compliance, 2(3).
- Sedona Conference. (2008). "Jumpstart Outline": Questions to ask your client and your adversary to prepare for preservation, rule 26 obligations, court conferences and requests for production, May 2008. Available online at www.thesedonaconference.org/dltForm?did=Questionnaire.pdf.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) **What is the meaning of E-discovery?**

Electronic discovery or “e-discovery” is the exchange of data between parties in civil or criminal litigation.

2) What are the objectives of EDRM?

The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;
b) Associate document collections with particular users (custodians);
c) Capture and preserve the metadata associated with the electronic files within the collections;
d) Establish the parent-child relationship between the various source data files;
e) Automate the identification and elimination of redundant,duplicate data within the given dataset;
f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;
g) Unprotect and reveal information within files; and
h) Accomplish all of these goals in a manner that is both defensible with respect to clients’ legal obligations and appropriately cost-effective and expedient in the context of the matter.

3) Write any 3 recommendations that are provided for investigators and in-house counsel to avoid the same fate as Qualcomm?

- Use checklists and develop a standard discovery protocol;
- Go to the location where information is actually maintained—do not rely entirely on the client to provide responsive materials to you;
- Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;

4) What are the five digital storage locations?

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB “thumb” drives

- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

1.11 ACTIVITY

Explain the meaning of electronic discovery and the violations with respect to it? Also, how it is utilized in the criminal procedure? Briefly explain it with relevant case laws? (800 – 1000 words)

Block 2

Cyber Forensics Process, Standards and Challenges

Unit 1: Digital Evidence and Processes involved in Digital Forensics

1

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Digital Evidence
1.4 Locard's Principle
1.5 Best Evidence Rule
1.6 Characteristics of Digital Evidence
1.7 Types of Investigation
1.8 Challenges in Digital Forensics in the present era
1.9 Processes involved in Digital Forensics
1.10 Role of First Responder
1.11 Let's sum up
1.12 Further reading
1.13 Check your progress: Possible answers
1.14 Activity

1.1 LEARING OBJECTIVES

After going through this chapter, you should be able to understand:

- Challenges in cyber forensics

- Principles in evidence management
- Role of First Responder

1.2 INTRODUCTION

The field of cyber forensics is still in its infancy stage as it possesses a strong need for direction and definition. Areas of speciality within a professional environment, certifications, and/or curriculum development are still questioned. With the continued need to standardize parts of the field, methodologies need to be created that will allow for uniformity and direction. To date, huge volumes of data, heterogeneous information and communication technologies, and borderless cyberinfrastructure create new challenges for security experts and law enforcement agencies investigating cybercrimes.[43] The future of digital forensics is explored, with an emphasis on these challenges and the advancements needed to effectively protect modern societies and pursue cybercriminals. Today the technology in cyber forensic is utilizing the application of scientific methods and technics to recover data from electronic and digital media. The increase in the growth of computer and the Internet use has changed the human behaviour and ways of communication, this growth in technology has given rise to the rise in cybercrime which is now sophisticated and difficult to trace, investigate, and prosecute of criminals without reliable and accurate data collection.[44]

1.3 DIGITAL EVIDENCE

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic if it is hearsay and whether a copy is acceptable or the original is required. The digital evidence is used to establish a credible

[43]ORGANIZING RESEARCH AND DEVELOPMENT IN CYBER FORENSICS <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1075&context=techmasters>
[44]Adelstein F (2006) Live forensics: diagnosing your system without killing it first. Commun ACM 49(2):63–66

link between the attacked, victim, and the crime scene. Some of the information stored in the victim's system is based on the IP address, system log-in & remote log-in details, browsing the history, log files, emails, images etc.

1.4 LOCARD'S PRINCIPLE

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing. Digital evidences must follow the requirements of the Best Evidence Rule.[45]

1.5 BEST EVIDENCE RULE

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

[45]Rahayu, S. &Robiah, Y. & Sahib, Shahrin.(2008). Mapping Process of Digital Forensic Investigation Framework. 8

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.[46]

1.6 CHARACTERISTICS OF DIGITAL EVIDENCE

The following are the essential characteristics of digital evidence:-

- ***Admissibility***

  It must be in conformity with common law and legislative rules. There must be a relationship between the evidence and the fact being proved. Digital evidence is often ruled inadmissible by courts because it was obtained without authorization. In most jurisdictions, a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another.[47]

- ***Reliability***

  The evidence must be from undisputed origin

- ***Completeness***

  The evidence should prove the culprit's actions and help to reach a conclusion.

- ***Convincing to Judges***

  The evidence must be convincing and understandable by the judges.

- ***Authentication***

  The evidence must be real and related to the incident. Courts largely concerned themselves with the reliability of such digital evidence. The investigator must be able to prove to the authenticity of the digital evidence by explaining:

- The reliability of the computer equipment.
- The manner in which the basic data was initially entered.

[46]Hewling, Moniphia&Sant, Paul. (2012). Digital Forensics: An integrated approach

[47] Carrier B. D., Spafford E, (2004) "An event based Digital forensics Investigation Framework"Center for Education and Research in Information Assurance and Security

- The measures taken to ensure the accuracy of the data as entered.
- The method of storing the data and the precautions are taken to prevent its loss.
- The reliability of the computer programs used to process the data, and
- The measures taken to verify the accuracy of the program.

1.7 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists.

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or privatecontractors working for them). Criminal forensics is usually a part of a wider investigationconducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

c) Electronic discovery (eDiscovery)

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical toits criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employeesnot to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) Intrusion Investigation

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation isinstigated as a response to a network intrusion, for example, a hacker trying to steal corporatesecrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

1.8 CHALLENGES IN DIGITAL FORENSICS IN PRESENT ERA

Digital forensics is facing a crisis. Hard-won capabilities are in jeopardy of being diminished or even lost as the result of advances and fundamental changes in the computer industry:

- The growing size of storage devices means that there is frequently insufficient time to create a forensic image of a subject device or to process all of the data once it is found.
- The increasing prevalence of embedded flash storage and the proliferation of hardware interfaces means that storage devices can no longer be readily removed or imaged.
- The proliferation of operating systems and file formats is dramatically increasing the requirements and complexity of data exploitation tools and the cost of tool development.[48]
- Whereas cases were previously limited to the analysis of a single device, increasingly cases require the analysis of multiple devices followed by the correlation of the found evidence.
- Pervasive encryption means that even when data can be recovered, it frequently cannot be processed.
- Use of the ***"cloud"*** for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot even be found.
- Malware that different programmed information to persistent storage necessitates the need for expensive RAM forensics.
- Legal challenges increasingly limit the scope of forensic investigations.

These problems are most obvious to examiners faced with cell phones and other mobile computing platforms. It is vital for forensics examiners to be able to extract data from cell

[48] Brill AE, Pollitt M (2006)The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1:3–11

phones in a principled manner, as mobile phones are a primary tool of criminals and terrorists. But there is no standard way to extract information from cell phones. In recent years there has been substantial interest in RAM-based forensics to defeat encryption and to find malware that is not written to persistent storage. RAM forensics can capture the current state of a machine in a way that is not possible using disk analysis alone. But RAM Digital Forensics tools are dramatically more difficult to create than disk tools. Unlike information written to disk, which is stored with the intention that it will be read back in the future possibly by different programmed information in RAM is only intended to be read by the running program. As a result, there is less reason for programmers to document data structures or conserve data layout from one version of a program to another. Both factors greatly complicate the task of the tool developer, which increases tool cost and limits functionality.

1.9 PROCESSES INVOLVED IN DIGITAL FORENSICS

The digital forensics process involves the following five levels of investigation:-

a) Identification of the Digital Evidence

This step involves the identification of any digital evidence which might be present at the crime scene. This can involve computers, pen drives, hard disks or any other electronic device that can store digital data. Also, it needs to be taken care of that the processes followed when the computer is found in on or off state are different.

b) Acquisition of the Identified Evidence

This step comes after the identification step as after the evidence has been identified it needs to be acquired in the most appropriate manner such that the integrity of the data stored in the evidence remains intact. The sub-steps followed during this part of the investigation can be seizing the crime scene, forensically acquiring the data stored in the found devices for further investigation. The two sources of evidence: ***volatile and non-volatile data*** have different methods of acquisition. In the case of volatile data, the order in which the data is collected is of utmost importance. One suggested order can be network connections, ARP cache, login session, running processes, open files and the contents of RAM. Meanwhile, in case of non-volatile data i.e. from hard-disk the bitstream image can be done using three strategies: using

a hardware device such as write blocker where the system is taken offline and the hard drive is removed, using a forensic tool Helix which is used to boot the system or using a live system acquisition which can be done either locally or remotely in case of encrypted systems that cannot be taken offline or are only accessible remotely.[49]

c) Preservation of the acquired evidence

The evidence acquired should be kept in such a way that it remains the same even after the investigation process has been completed as it was first acquired. This is done via a well-defined process known as the chain of custody which ensures that the evidence remains protected from the unintended alterations. In order to achieve this, read-only copies are made by the practitioners or experts to work upon whereas, the original evidence is kept in a secured location.

d) Examination and Analysis stage

This is the most crucial step of any investigative procedure as it is the strongest as well as the most vulnerable part where any minor mistake can lead up to the evidence's ineffectiveness to be presented in the court of law. Examining the evidence involves the step of categorizing the digital evidence and the tools which would be used to analyse that evidence. For instance, a received email can include multiple information regarding the source's email address, metadata as well as the data which can be used to find the IP address of the sender's workstation. One important advice which needs to be taken care of at this stage of analysis involves the difference in the data generated from different devices. For instance, the data and the metadata generated from an image and an email would be different. Evidence's correctness and authenticity to be presented in the court of law totally depends upon the expert's experience and skill.

e) Presentation or Documentation of Evidence

This is the last stage of the investigation procedure which includes the process of presenting a report or documentation on what type of evidence was obtained, the description about the experts who worked upon the evidence, the methods followed and the tools used in a specific

[49]Carrier, B, &Spafford, E H (2004) An Event-based Digital Forensic Investigation Framework.Proceedings of Digital Forensics Research Workshop. Baltimore, MD

format. The report can also include the protocols and legal policies followed. It should be presented in the most understandable way stating its findings to be very accurate.

1.10 ROLE OF FIRST RESPONDER

The first responder is the person who first accesses the victim's computer. He must be prepared well to collect the evidence for the crime scene in a manner that is accepted by the court.[50] Therefore, the availability of trusted digital forensics toolkit is necessary for the first responder. Some of the important steps in preparing the first responder's toolkit are:

a) Create a forensics tool testbed

The testbed should be created from the trusted source and functionality of the testbed should be checked in advance before using them in the field. Some of the guidelines are:

- Identify the appropriate OS type your organization is using, based on which the testbed is created. An organization may have a verity of OS deployed in its network. For example, it may have Linux based servers and Windows and Mac-based PC/Laptop. In that case, one has to create multiple testbeds for each OS type.
- Disinfect the testbed from the availability of any data on the machine. Preferably use a new/fresh machine. In case, a new machine is not available to use wiping tools to wipe out any data from the machine.[51]
- Install the OS and all the necessary software to conduct the forensic investigation.
- Ensure that the OS and all the programmes installed in the testbed are updated to the latest version. If any patch is required for the successful operation of the system, the same should also be installed.
- Compute Hash to ensure the integrity of the file system.

b) Document the Forensics tool testbed

It includes the following:-

- Name, type and version of OS.

[50] Casey, E (2004) Digital Evidence and Computer Crime (2 ed) Elsevier Academic Press

[51] K.Rogers, M., Goldman, J., Mislan, R, Wedge, T, &Debrota, S (2006) Computer Forensics Field Triage Process Model. Proceedings of Conference on Digital Forensics, Security and Law, (pp 27-40)

- Details of the types of various applications/software installed in the testbed along with the details of the upgrades and patches.
- Details of various types of hardware installed in the testbed.
- Details pertaining to hash and checksum of the testbed.

c) Document the summary of the forensic tools

For every tool that is acquired for the testbed, the following information is documented for easy reference and record.

- Details about the source from where the software was brought. In case it's a freeware, mention the site/source from where the tool was downloaded.
- Detailed description about the purpose, working and compatibility of the tool with OS and other software.
- Details of tool dependencies and the system effects which include the details about the required system access levels by the user to run a tool and the details of shared libraries.

d) Test the tools

Now the tools selected and installed are tested in the testbed and its performance and output is examined.

1.11 LET'S SUM UP

In this chapter, we have studied digital evidence and its characteristics along with the best evidence rule. Finally, we also studied the challenges faced in digital forensics in the present era and the processes involved in digital forensics.

1.12 FURTHER READING

- Rahayu, S. &Robiah, Y. & Sahib, Shahrin. (2008). Mapping Process of Digital Forensic Investigation Framework. 8.
- Adams, Richard & Hobbs, Val & Mann, Graham. (2014). Journal of Digital Forensics, Security & Law. Journal of Digital Forensics, Security & Law. 8. 25-48.

- Hamidovic, Haris&Salkic, Hadzib. (2016). THE BASIC STEPS OF DIGITAL EVIDENCE HANDLING PROCESS. International Journal of information and communication technologies. 2.
- Prasad, Ajay &Pandey, Jeetendra. (2016). Digital Forensics.

1.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Locard's Principle?

Wherever a criminal, steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. Digital evidence is usually not in a format that is directly readable by a human. Therefore it requires some additional steps to convert it into a human-readable form in the form of writing.

2. What are the different types of investigation?

There are four main types of investigation performed by digital forensics specialists.

a) Criminal Forensics

Criminal forensics is the largest form of digital forensics and falling under the remit of law enforcement (or privatecontractors working for them). Criminal forensics is usually a part of a wider investigationconducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a layman will understand.

b) Intelligence gathering

Intelligence gathering is a type of investigation associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used before the court of law, forensic soundness is less of a concern in this form of investigation, instead of speed can be a common requirement.

c) Electronic discovery (eDiscovery)

Electronic discovery or eDiscovery is similar to ***"Criminal Forensics"*** but in relation to civil law. Although functionally identical toits criminal counterpart, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employeesnot to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

d) Intrusion Investigation

The final form of investigation is different from the above-mentioned three types of investigation. Intrusion investigation isinstigated as a response to a network intrusion, for example, a hacker trying to steal corporatesecrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hacker's activities. Intrusion investigation often occurs ***"live"*** (i.e. in real-time) and leans heavily on the discipline of network forensics.

3. What is Best Evidence Rule?

The Best Evidence Rule, which has been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

1.14 ACTIVITY

Explain the challenges and the process involved in digital forensics along with the Role of the First Responder and the important steps in preparing the toolkit? (1000-1500 words)

Unit 2: Overview of First Responder 2

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Phases of Cyber Forensic Investigation

1.3 Forensic Duplication

1.4 Introduction to First Responder

1.5 First Responder Toolkit

1.6 First Responder Basics

1.7 First Responder Procedure

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Understand Cyber forensics investigation Phases
- The process of forensic duplication
- Role of First responder ,its toolkit and procedure

1.2 PHASES OF CYBER FORENSIC INVESTIGATION

We all know that cyber forensics is a branch of forensic science which mainly includes the different stages of digital evidence namely Identification, Acquisition, Analysis and Presentation.[52]

Despite these stages, there are different phases of cyber forensics. Lets' us understand every phase in detail.

1. **PLANNING**

   In this phase, investigator does all the necessary arrangement to carry out the actual forensic investigation. This phase mainly consists of requirement and information gathering. This phase ensures high quality investigations output. In this phase, the forensic investigator gathers all related information of the incident actively and passively. He also prepares toolkit required for the investigation by understanding the scope. The forensic investigator obtains permission from authorities to conduct further steps. This permission is formerly known as Search Warrant. With the proper execution of the planning phase, the forensic investigator gets in-depth knowledge of facts of the case which is required to decide further approach. The key elements of this phase are interviewing the victims, identifying affected computing devices and deciding the digital forensic procedure to be used. In this process, the forensic investigator has given instructions, clarification and guidelines for performing activities. Allocation of roles and resources is been decided in this phase. Obtaining approval for forensic investigation is the key factor of this phase.[53]

2. **SEARCH AND IDENTIFICATION**

[52] Nelson, Bill. Guide to Computer Forensics and Investigations. Boston, MA: Thomson Course Technology, 2004 (ISBN 0-619- 13120-9)

[53] National Institute of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement <http://www.ncjrs.org/pdffiles1/nij/199408.pdf >

This phase mainly deals with identifying the affected people and the infrastructure of the given incident. This can be done effectively with the proper inputs obtained from the previous phase. Different tools and methods can be used to identify the type of attack. Search facilitates examination of the suspected people as well as systems. This phase also contributes to deciding the scope of the overall investigation. Proper approval is a necessity to conduct this phase. The output of this phase clarifies the number of people and the system to be examined in further investigation.

3. SEIZER

This phase starts with securing the crime scene. Before the actual examination of digital evidence in the forensic lab, it should be properly seized. There are different seizer procedures for different types of evidences. As per the requirement, scientific and legal seizer procedure is used like Isolation of system from the network, a photograph of the running machine skill. Applying forensic shutdown processes. Removing storage media like hard disk, memory card without any damage etc. The seizer memo is been created which is signed by the investigator and the witnesses. Seizer memo contains a brief description of evidence and procedure followed to seize particular evidence. The digital evidence collection form is been also prepared and filled accordingly for the sized evidence.[54]

4. ACQUIRE

The acquisition phase mainly consists of bit by bit forensic disk imaging, disk cloning, taking memory dump and creating evidence file suitable for analysis purpose. The hardware and software write blockers are used in this process to avoid any unintentional alteration or modification in digital evidence. To ensure the admissibility and integrity of the evidence a hash value is been calculated in this phase. There are different forensic tools available for different evidences to acquire entire evidence in a forensic manner.

[54]National Institute of Standards and Technology. CFTT Methodology Overview <http://www.cftt.nist.gov/Methodology_Overview.htm>

The acquisition can be physical or logical. In a physical acquisition, the entire disk is been acquired. In a logical acquisition, logical partition of the disk is been acquired. In both cases write blocker are required. In this process, copies of evidence are made and its hash value is been verified.

5. COLLECT AND PRESERVE

In this phase, sealing, labelling and bagging of the evidence is been done at the crime scene. At most care is been taken while packing digital evidences is been taken in order to avoid physical damage during transportation. Chain of custody document is been created and properly filled. This document gives the information regarding accountability of the evidence in terms of who, when, why and for how much duration was handling that evidence. Properly sealed evidence is been created and preserved in an evidence storage box. The preserved evidence will be further transported to the location where the actual analysis will be carried out.

6. ANALYSIS

The acquired information needs forensic examination. When the evidence is been transported to the forensic lab before analysis, the hash value is been verified by the forensic experts. This helps to prove the integrity of digital evidence before analysis. Every file out there is with some purpose and proper analysis of the available data can reveal many ways to proceed in further investigation. For the said purpose, the appropriate techniques and tools need to be used to make a relevant mole-hill out of the mountain of the data, consistently yielding exemplary and concise results.

The examiner may use additional tools to recover deleted information. The used tools must be validated to ensure their reliability and correctness. Forensic expert analyze the evidence twice to verify the correctness of the findings. During analysis, the evidence found is been assembled to reconstruct event or actions to provide the facts.

7. REVIEW AND REPORT

After the examination is complete, the findings are reviewed and documented in the report. It includes a detailed description of the conducted steps during the investigation. The examination report typically contains following details:

Name of the examiner who did the examination, Date and time when is been done, Software and hardware that were used, their version numbers, Hash value verification and related clicked photographs.

The information related to the acquired evidence such as hard disk and mobile device details should be also included. The report generated should be easy to understand and explain in precise details. Further actions are determined after the report is reviewed

8. PRESENTATION

Presenting an understandable, defendable and complete report is the key to gettingthe desired outcome of the whole process. Expert witness testimony is one of the most important tasks of presentation finding. Success of the forensic investigation is very much dependent upon the way it has been presented and defended in a court of law.

1.3 FORENSIC DUPLICATION

Forensic duplication refers to bitstream imaging of data from the digital media in question. Data resides in all sorts of storage media present in computers, smartphones, GPS devices, USB drives, and so on.[55] We need to be able to get to this information in a manner that it does not change the information on the devices themselves. If the evidence is not collected properly, we face an issue where the results of the forensic exam will be put in doubt. Hence it is necessary to copy the data carefully in a forensically sound manner.

LOGICAL BACKUP	BITSTREAM IMAGING
A logical backup copies the directories and files of a logical volume. It does not capture	Also known as disk imaging/ cloning/ bitstream imaging generates a bit-for-bit copy

[55] Kruse, Warren G., Heiser, Jay G.; Computer Forensics: Incident Response Essentials, Addison Wesley, Boston, Massachusetts, September 2001, ISBN: 0-201-70719-5

other data that may be present on the media, such as deleted files or residual data stored in slack space.	of the original media, including free space and slack space. Bitstream images require more storage space and take longer to perform than logical backups.

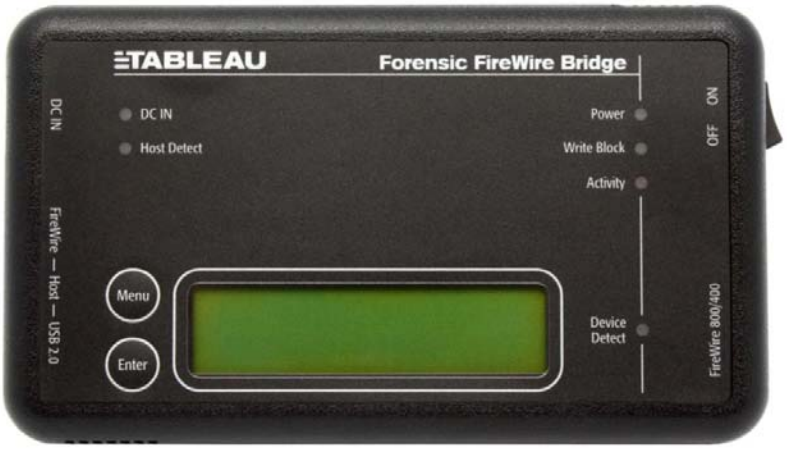
The Important thing required for forensic Investigation is Write blocker

WRITE BLOCKER

A write-blocker is hardware or software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.

Features:-

- Prevents any writes to the seized media
- Suspect hard disk connected to the forensic computer via a write blocker



Things to understand and remember about Digital evidence

- Almost every type of crime has digital evidence in it.
- The investigator must apply the same level of maturity, knowledge, security and safety while dealing with digital evidence likewise other traditional evidence

- Nature of Digital Evidence is delicate and fragile. Hence improper handling may result in damage or tampering of the evidence.
- Digital Evidence can be easily altered or manipulated without intention
- Never Assume Digital evidence is destroyed completely

RULES OF DIGITAL FORENSICS

- Never work on original evidence.
- Never mishandle evidence.
- Use proper software utilities to retrieve evidence from the media.
- Document everything while handling the suspected media.[56]

THE FOUR PRINCIPLES FOR THE AUTHENTICATION AND INTEGRITY OF EVIDENCE ARE

PRINCIPLE 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

PRINCIPLE 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

PRINCIPLE 3:

An audit trail or another record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

PRINCIPLE 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

HASHING

Hashing is a process of converting large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.[57]

[56]Mandia, Kevin, Prosise, Chris; Incident Response: Investigating Computer Crime, New York, 2001, ISBN: 0-07-213182-9

Salient features of the process of the hashing

- The integrity of the seized evidence through the forensically proven procedure.
- Produces fixed length unique value representing the data on the seized media.
- Any changes in the evidence will result in a change in the hash value
- Hashing is a process of converting the large, possibly variable-size amount of data into a small datum by well-defined procedure or mathematical function.
- Hashing is mainly done to check the integrity of the data.
- Values returned after hashing is commonly called as hash values, hash sums or hashes
- Commonly used Hash functions are
- MD5 Hash Algorithm
- SHA1 Hash Algorithm
- While imaging the original Hard disk, a hash value is generated.
- After imaging,the hash value will be generated.
- The hash value of the original Harddisk = Hash value of the imaged Hard Disk, then we can say that the Message integrity is 100%

Commonly used Software for Imaging will calculate this Hash Values. Say for example

1. C-DAC's Cyber Check Suite
2. FTK Imager
3. Win Hex
4. Encase

1.4 INTRODUCTION TO FIRST RESPONDER

The first responder is the person who plays a vital role in the overall investigation. The tasks performed by the first responder are very much crucial for the investigation. Any mistake by the first responder may lead to tampering of the evidence or wrong direction of the investigation. Hence, the first responder is very much responsible for the further success of the investigation. The first responder is defined as a person who arrives first at the crime scene and accesses the

[57] Nelson, Bill; Phillips, Amelia; Enfinger, Frank &Steuart, Chris; Guide to Computer Forensics and Investigations, Boston, Massachusetts, Course Technology, 2004, ISBN: 0-619-13120-9

victims computing devices after the incident. Protection, Integration and Preservation of the digital evidence are the key responsibilities of the first responder. He may be network administrator, investigation officer, law enforcement officer etc.[58]

Following are the important roles of First Responder:

- Identify the crime scene, affected people and affected computing devices.
- Protect the identified subject of the crime scene.
- Preserve the temporary and fragile evidence.
- Gather detailed information about the incident.
- Document all the findings.
- Seizer of the identified Digital Evidences.
- Package and transport of the Digital Evidence.

1.5 FIRST RESPONDER TOOLKIT

First Responder Toolkit defined as a collection of tools required to seize digital evidence in a genuine and presentable way. The toolkit helps First Responder to understand the limitations and capabilities of digital evidence at the time of collection.

The first responder is responsible to select a trusted forensic tool that gives the desired output. While creating first responder toolkit, the tools must be tested and validated before actual use. The details of every tool should be documented. Along with version name and hardware requirements. Multiple tools for similar functionality should be available in the toolkit. First responder toolkit should consist of a collection of following a different set of tools.

Disassembly Tools- Screw Drivers, Wire Cutters, Tweezers etc.

Documentation Tools- White Papers, Markers, Tag, Stick-on papers etc.

Packaging Tools- Evidence Bags, Bubble Wrap, Tape, Cable ties, Anti-static bubble wrap, Anti-static bags etc.

[58] US Department of Justice; Electronic Crime Scene Investigation: A Guide for First Responders, Washington D.C., July 2001, NCJ-187736<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>

Forensic Equipment- Bootable Disk, External Hard Drives, Pen Drives, Write Blockers, Data Acquisition Software and Hardware field response Kit.

1.6 FIRST RESPONDER BASICS

THERE ARE SOME GROUND RULES OF FIRST RESPONSE[59]

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

1.7 FIRST RESPONDER PROCEDURE

Following are different steps which should be taken by the first responder.[60]

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

[59]<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf>
[60]<https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

SECURING CRIME SCENE

It is important to follow a certain procedure in order to secure the crime scene. Properly secured crime scene help forensic investigator to carry out further tasks.

Following are some guidelines to the first responder in order to effectively secure the crime scene.

a. Understand and verify the type of incident and prepare accordingly.
b. Make sure that the premise is safe for investigators.
c. Find and help the victim.
d. Ensure that nobody will access the computer systems by isolating the people out there.
e. Document all connection of the suspected device and disconnect to make the system stand alone.
f. Observe the situation at the crime scene and note down all these observations.
g. Protect the fingerprints that can be found on the suspected computing devices.
h. All the forensic investigator should wear hand gloves and anti-static wrist belts.

COLLECTING PRELIMINARY INFORMATION

In order to collect initial information, the interviews of the related people should be carried out. For that questionnaire according the incident needs to be prepared. Search warrant act as permission to conduct the interviews. If required the written consent of the interviewer should be obtained before the interview. If required witness signature can also be obtained over the important documents such as search warrant, consent form etc. While conducting interviews different question should be asked to get detailed knowledge about certain facts e.g. owner and

user of the computing device, internet service provider, purpose of using the system, offsite data storage, password required to access system software or data etc.

The first responder can also create a checklist of the expected information which needs to be collected as per the type of the incident.

Following are some of the key questions which should be discussed during this phase of the investigation.

- What steps were taken to contain the issue?
- Were there any logs (system access, etc.) present that cover the issue?
- Are there any suspicious entries present in them?
- Did anyone use the system after the issue occurred?
- Did you observe any similar instance before?
- Were there any alarms that were set off by the firewall/IDS/network security devices?
- Please give detailed documentation on the set of commands or processes run on the affected system or on the network after the issue occurred.
- Do they have similar systems in any of the branch/other offices?
- Whether log register of the Internet users/other users is maintained?
- Are there any questions about the issue that have not been answered?

At the scene of the offence, IO should gather the following information during the interviews phase

- Identify the complainant/owner (s) of the various devices and obtain the access details, usernames, and service providers' details.
- Gather information as provided in the questionnaire(s) above, on all the security systems.

- Identify the list of the people who can identify the network and a schematic diagram of the network.

DOCUMENTING THE SCENARIO

It is important to create certain records by documenting the crime scene. This may give certain findings which can be used further. All the observation of the crime scene should be properly documented such as the position of the screen, mouse and other components of the system. Listing down all the components and its connections help to understand the technique used by the criminal. Documenting also includes a detailed description of different facts of computing devices such as power status, storage devices etc. Photograph of the screen of running computing devices should be clicked and write down the notes of the observations in it. A video camera can be used to capture the entire scene of the crime. A still camera should be used to take the photographs of the important object at the crime scene. Photography helps to notice even the smallest piece of evidence. In the documentation of the crime scene, sketches should be drawn for the layout of the area.

COLLECTING AND PRESERVING EVIDENCE

Nowadays there are many storage media available. As an Investigator one should know where the Digital Evidence is.The investigator should not ignore even a small piece of paper. It may contain valuable information that can be a Substantial Evidence to catch hold a criminal or culprit. This is a very important task for the Investigator.[61]

List of Storage Device to be collected from the scene of the offence

- CPU
- Hard Disk
- Floppy Drive
- CD's & DVD's Drive

[61]<https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types>

- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives

The very important stage of Investigation is to isolate all the Memory Components from the Computer or computer Network. That simply means making computer Standalone. This has to be done in order to avoid manipulation, alteration or deletion of Digital Evidence. As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.

PACKAGING AND TRANSPORTING EVIDENCE

PACKAGING

Following are the important points to be considered while packaging the evidence.

- Evidence should be properly documented
- The evidence should be labelled as per the type of evidence.
- The evidence should be inventoried
- Evidence should always be packed in antistatic packaging.
- Avoid folding, bending, or scratching the evidence.
- Seized / Confiscated Material should be properly packed in the box.
- Place labels (Exhibit No :) on the top of the package
- Check the size of the Hard Disk before seizing.
- Bring One Blank hard disk with the exact capacity (or more) that of suspect's HDD for forensic duplication process.

TRANSPORTATION

- The utmost care has to be taken while carrying the Seized components from one place to another.

- Ignorance while transportation may lead towards Tampering of Evidence
- Due to the sensitive and fragile nature of the computer evidence, place the computer in a box properly cushioned with non-static material.
- All the Seized Components should be packed with proper Packing material (Cello Tape, Boxes, Anti-Static Bags, Thermacol etc.)
- The Components should be kept properly.
- Store the computer is secure and dust-free place.
- The storage should not come in contact with water.
- Vibration Free Transportation.
- Evidence should not be kept in contact with any Electro-Magnetic field.
- As far as possible cover the mouse and keyboard with polythene covers to preserve fingerprints.
- Don’t bend the Pen drives, Floppy, CDs etc.
- Don’t place labels directly on Floppy drive/CD.
- Store it in normal temperature.

CRIME SCENE REPORTING

In order to explain what exactly has happened during the investigation, the investigator should document all the actions performed over the evidence. The overall responsibility of any changes in the evidence goes with the forensic investigator. Hence, the proper documentation is very much an important aspect of digital forensics.

Following are some of the key documents which every investigator should create during his investigation.

- Search warrant

- Chain of custody
- Digital evidence collection form
- Digital forensic report

Preparing a good and admissible report is the skilful work and the most important phase of the forensics process. The investigator's knowledge is judged by what he writes. The court cases can be won or lost because of the reports and its quality. Hence the investigator should have the knowledge to represent the facts and findings in a simple and understandable manner through the report. The report should be written in such a way that it should speak for the investigator for itself and it will exist as an official record for that case.

SALIENT FEATURES OF GOOD REPORT

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.8 LET'S SUM UP

In this chapter, we have studied the different phases of cyber forensic investigation along with forensic duplication. We also studied the basics and toolkit of First Responder and have ended our discussion with the First Responder Procedure.

1.9 FURTHER READING

- "Electronic Crime Scene Investigation – A Guide for First Responders" by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- Mugisha, David. (2019). ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS. International Journal of Cyber Criminology. 47. 3.
- Resources.sei.cmu.edu (2019), https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf (last visited Nov 25, 2019).
- Ncjrs.gov (2019), https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (last visited Nov 25, 2019).

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the different phases of cyber forensic investigation?**

    - Planning
    - Search and Identification
    - Seizer
    - Acquire
    - Collect and Preserve
    - Analysis
    - Review and Report
    - Presentation

2. **What are the ground rules of the first responder?**

Rule 1- The first responder must be competent and experience in handling technological gadgets.

Rule 2- The first responder should not do any such act which may tamper the digital evidence. The first responder should have knowledge of data acquisition technique mainly imaging and cloning.

Rule 3- He should secure the crime scene and maintain a secure state until the forensic team advises.

Rule 4- He should never take help of suspect to access the computing devices which may hold possible digital evidence.

Rule 5- He should document all the details of the crime scene and handed over those notes to forensic experts.

3. **What are the steps that needs to be taken by the first responder?**

Following are different steps which should be taken by the first responder.

Step 1. After planning for search and seizer and obtaining search warrant the first responder should secure and evaluate crime scene and conduct the initial search.

Step 2. In order to gather information regarding the incident, the first responder supposed to conduct the interviews.

Step 3. The first responder needs to photograph the crime scene and draw sketches of the scene.

Step 4. The first responder needs to document all the findings and create a note of it.

Step 5. The first responder needs to remove the storage device and note down its details.

Step 6. The first responder needs to exhibit numbering to the seized evidence and preserve them.

Step 7. Packaging and selling of the collected evidence should have been properly carried out with labelling upon it.

Step 8. The first responder should make sure that the evidence will be transported to a forensic lab safely.

4. **What are the salient features of a good report?**

- It perfectly describes the incident and its details
- It should be easy to understand by decision-makers.
- It gives a clear picture of the investigation without any open-end conclusion.
- It defines the proper timeline of the investigation.
- It omits irrelevant information.
- It clearly states what the investigator has done, which facts are uncovered and how these facts lead to the final conclusion.
- It provides supporting material such as equation, data, tables and figures.
- Anyone who is new to the situation should be able to understand it through the report.

1.11 ACTIVITY

Briefly explain the procedure that needs to be undertaken by the First Responder along with a case study? (1000-1500 words)

Unit 3: Evidence Management and Anti-Forensics

3

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Digital Evidence
1.3 Difference between physical and digital evidence
1.4 Sources of Digital Evidence
1.5 Seizure Proceeding
1.6 Challenges to forensics
1.7 Introduction to Anti-forensics
1.8 Definition
1.9 Primary goals of Anti-forensic
1.10 Types of Anti-forensic techniques
1.11 Conclusion

1.12 Let's sum up
1.13 Further reading
1.14 Check your progress: Possible answers
1.15 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you will be able to understand:

- Difference between physical and digital evidence
- Detail procedure of seizure proceedings by Investigation officer
- What are challenges to cyber forensics
- Definition of Anti-forensics and its types

1.2 DIGITAL EVIDENCE

In this chapter, we will understand the different basic concepts related to the entire technical investigation of digital evidence and its management.

Digital evidence or electronic evidence is ***"any probative information stored or transmitted in digital form that a party to a court case may use at trial".*** Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines"

1.3 DIFFERENCE BETWEEN PHYSICAL AND DIGITAL EVIDENCE

Digital Evidence	Physical Evidence

It can be duplicated and the duplicated copy can be analyzed as if it was original.[62]	It cannot be duplicated as Digital Evidence
Modification or Tampering of Digital Evidence can be easily identified by using appropriate Software by comparing with the original.	If any modification or Tampering is done it would be highly difficult to identify the changes happened.
It cannot be destroyed easily. Even if the evidence is destroyed, recovery is possible(not all times)	If the Evidence is destroyed it is highly impossible to bring back to its original form.
It facilitates working on duplicate copies of the digital media, original along with copies will still remain to help the investigators in the event of damage to the copies.	Since duplication is not possible, once the evidence is destroyed, the evidence cannot remain.
Less Tangible when compared with physical evidence	Tangible in nature

1.4 SOURCES OF DIGITAL EVIDENCE

Following are the different sources of digital evidence:-

[62]Scientific Working Group on Digital Evidence (SWGDE) of the National Center for Forensic Science (NCFS). Best Practices for Computer Forensics V2, 2006a. Retrieved From the World Wide Web on 07/07/12: URL <http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20V 2.0.pdf>

VOLATILE EVIDENCE

Volatile data will include information about the running process, network connections, clipboard contents, and data in memory.[63]

Volatile Evidence can be found on:

- Ram Memory
- Temporary file System / Swap Space
- Cache Memory etc.

NON-VOLATILE EVIDENCE

The data can be retrieved even when the computer is switched off.

Examples of Non-Volatile Data commonly includes:

- Flash Memory
- Hard Disk, Magnetic Tape
- Optical Disc etc.

Examples of digital evidence:

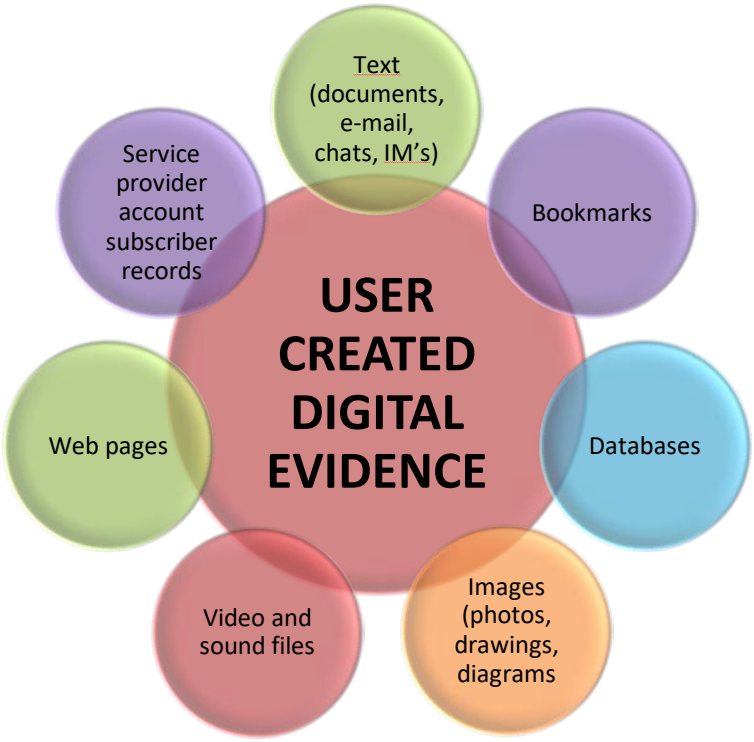
- Emails
- Web Server Logs
- Digital Photographs
- ATM Transaction logs
- Word processing documents
- Instant message histories
- Files saved from accounting
- Programs
- Spreadsheet
- Internet browser histories
- Databases,

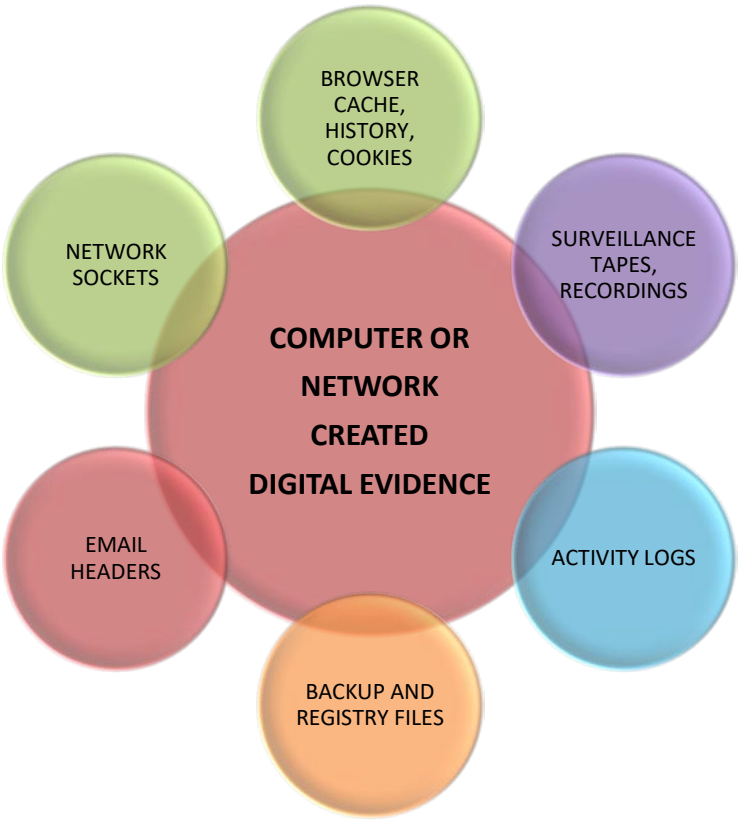
[63] Mason, D, Carlin, A, Ramos, S, Gyger, A, Kaufman, M, Treichelt, J, (2007)Is the open way a better way? Digital forensics using open source tools.The Computer Society. 1-10

- The contents of Computer Memory,
- Computer backups,
- Computer printers
- Global Positioning System tracks,
- Logs from a hotel's electronic door locks,
- Digital video or audio files.

We can categorize digital evidence in two main subcategories:-

1. User-Created digital evidence
2. Computer Created Digital evidence





1.5 SEIZURE PROCEEDINGS

Following is the probable list of equipment's which can be seized in technology-based crimes

- CPU
- Hard Disk
- Floppy Drive
- CD's & DVD's Drive
- USB Memory Sticks
- Pen Drives
- Memory Cards
- Portable Hard Disks
- Tape Drives
- Various Hi-Tech Gadgets
- & in some cases Cell phone / Mobile Handset

PANCHANAMA (SEIZURE MEMO)

The legal provisions empowering the investigation officer to conduct search and seizure are provided under section 165Cr PC and section 80 of the ITAA 2008.Panchanama and seizure procedure is as important in cybercrime investigation as in any other crime. Make sure one of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings, to identify the equipment correctly and to guide the IO and witnesses.[64] Please refer to the notes made during the pre-investigation assessment for cross verifying and correctly documenting the technical information regarding the equipment, networks and other communication equipment at the scene of the crime.Time Zone/System Time Play a very curtail role in the entire investigation. Please make sure this information is noted carefully in the panchanama, from the system that is in "switch on" condition. Please Don't switch On any device. Please make sure serial number is allotted for each device and the same should be duly noted not only in the panchanama but also in the chain of custody and digital evidence form.[65]Make sure each device is photographed before starting of the investigation process at their original place along with a respective reference.Make sure the photograph hard disk drive or any other internal part along with the system, once removed from the system

Capture the information about the system and dada you are searching and seizing in the Panchanama .Brief the witnesses regarding the tools used to perform search and seizure of digital evidence

Hence following are the important points to be considered while drafting a seizure memo.

- Power to search, seize under Section 165 Cr PC and, Section 80 of the ITAA 2008.
- Independent Witnesses.
- Time Zone/System Time
- The serial number for each seized device
- Chain of Custody & Digital Evidence Collection forms

DIGITAL EVIDENCE COLLECTION FORM

[64] Kruse W Heiser J G (2001) Computer Forensics: Incident Response Essentials (1st ed), Addison Wesley Professional. USA

[65] Casey, E (2004). Digital Evidence and Computer Crime, Forensic science, Computers and the Internet. Academic Press, London, UK

Digital Evidence Collection form is one of the most important elements of the forensic process. It is necessary that the steps taken for collection should be accurate and repeatable with the same results every time it is done. For this to happen, proper documentation of the process used for collection needs to be maintained for every device that is collected. This documentation should contain all the information about the evidence that is visible to the naked eye. It should contain information about the kind of software and version used and the time when the collection process started and ended. This documentation called as the Digital Evidence Collection (DEC) form thus consists of the information on the evidence and the media on which the evidence is being copied to.[66]

DIGITAL EVIDENCE COLLECTION (DEC) FORM SHOULD HAVE THE FOLLOWING FIELDS

- System Information
- Type — Device type which is produced to extract evidence like desktop, laptops, etc.
- Manufacturer — The device manufacturer information to be documented.
- Model Number — The device model number information to be documented.
- Serial Number / any unique identification feature — The device serial number information to be documented.
- BIOS Date/Time — BIOS information of the device.
- Property Form Number / Evidence Number — Unique number assigned to each device for easy identification by the unit after it is brought to the police station/unit.
- It is one most important element of the forensic process.
- Proper documentation of the process used for the collection of evidence must be maintained for every device collected.
- This document should contain all information about the evidence visible to naked eye
- It should contain information about the kind of software and version used and the time collection process started and ended.
- During the process of digital evidence collection, if the IO is trained or has a technical expert to support him, He should forensically image the evidence and acquire the hash value and note the same in DEC form as well as in panchanama.

[66]Cuardhuain S O, (2004) An Extended Model of Cyber Crime Investigation Journal of Digital Evidence. Vol 3 Issue 1

- The process, the tool and the hashing algorithm used should be reflected in DEC form the report generated by forensic tool should form as an enclosure to DEC.

CHAIN OF CUSTODY

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analysing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the Concerned person.[67]

- It refers to the documentation that shows the people who have been entrusted with the evidence.
- These would be people who have seized the device-
  - people who are in charge of transferring the evidence from the crime scene to forensic lab,
  - people in charge of analysing the evidence and so on.
- Due to the sensitive nature of digital evidence, it necessary to know who, when, what, where, and why was the evidence transferred to the concerned person.
- It is difficult to prove the integrity of the evidence if the chain of custody is not properly maintained.
- Lack of integrity in the process of custody and absence of appropriate documentation in this regard, will not be detrimental to the cybercrime investigation, during the trial but also, exposé the IO's to criminal liability under section 72 of the ITAA 2008.

IMPORTANT POINTS TO CONSIDER FOR CHAIN OF CUSTODY

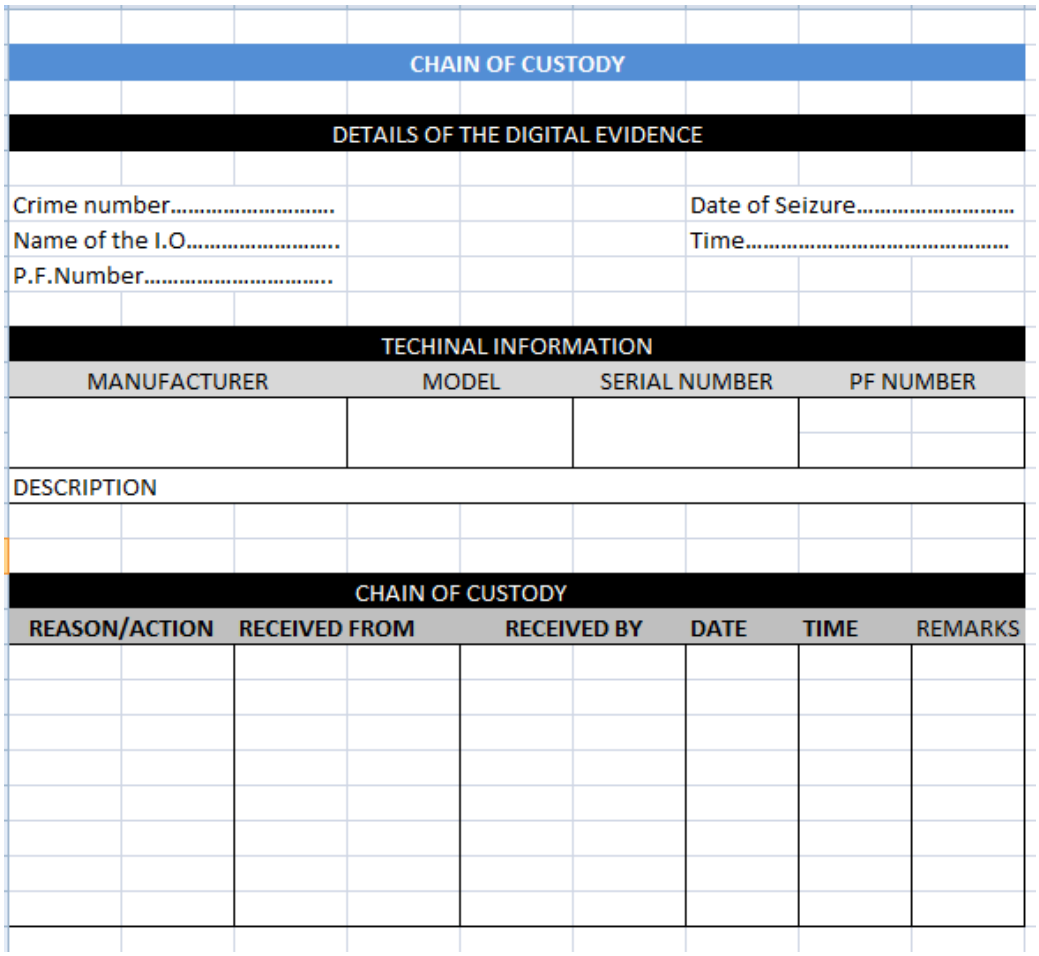
- Physically inspect the storage medium – take photographs and systematically record observations[68]
- Guard against hazards like theft and mechanical failure.

[67] Yong-Dal S, (2008) New Digital Forensics Investigation Procedure Model. Proceedings of Fourth International Conference on Networked Computing and Advanced Information Management. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4624063>

[68] Kuchta K J, (2000) 'Computer Forensics Today Law, Investigations and Ethics Available from: <http://www.liv.ac.uk/library/ohecampus/>

- Use good physical security and data encryption.
- Keep multiple copies in a different location.
- Protect digital magnetic media from external electric and magnetic fields.
- Ensure protection of optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and the data to a minimum.
- Always accompany evidence with their chain of custody forms.
- Give the evidence positive identification all the times i.e. legible and written with termagant ink.
- Establishing the integrity of the seized evidence through the forensically proven procedure by a technically trained IO.
- The seized original evidence can be continued to check for its integrity by comparing its hash value to identify any changes to it.

FORM



CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number..... Date of Seizure.....

Name of the I.O..... Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

1.6 CHALLENGES TO FORENSICS

The Direct Challenge to forensic is the use of anti-forensics by the attacker. In this chapter, we will see the different methods by which the forensic investigation process may become difficult for the investigating officer.

1.7 INTRODUCTION TO ANTI-FORENSICS

The objective of cyber forensics is to collect, analyse the evidence from the seized devices in such ways so that they are admissible in a court of law. There are many computer criminals are aware of this issue. They try to find a countermeasure technique and even developing tools

specifically designed to conceal their activities and destroy digital evidence. Anti-forensics is a collection of tricks and techniques that are used and applied with the clear aim of forestalling the forensic investigation. Anti- forensics works in the exact opposite direction of the cyber forensics. These methods make investigation much time consuming or more expensive to carry out.

1.8 DEFINITION

Harris (2006) stated that anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

Pajeket all (2012) defining the methodologies used against the computer forensics processes are collectively called Anti-Forensics.[69]

John Barbara defines anti-forensic as an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time-consuming, or virtually impossible.

1.9 PRIMARY GOALS OF ANTI-FORENSICS

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.
- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.10 TYPES OF ANTI-FORENSIC TECHNIQUES

[69] Liu, V, & Brown, F. (2006, April 3). Bleeding-Edge Anti-Forensics.Presentation at InfoSec World 2006. Retrieved September 11, 2007, from <stachliu.com/files/InfoSecWorld_2006-K2-Bleeding_Edge_ AntiForensics.ppt>

In order to act against the forensics one has to have sound knowledge of cyber forensics. The basic stages involve in cyber forensics are identification, collection, preservation, analysis and presentation to make digital evidence admissible in a court of law. So, basically all kind of anti-forensic technique is trying to break in one of this stage.[70]

CREATING PROBLEMS AT THE EVIDENCE SOURCE

This technique is used to create more hurdles for a forensic investigator. It may result in time increased for analysis of the evidence. Sometimes this technique does not let computing device create any logs or the traces related to any event over the device. This technique also suggests permanent deletion of the information within the device. Following are some of the methods used to apply this technique

A. ***Disk Wiping*** **-** Data can be still recovered if it is a normal delete over computing device. Hence disk wiping technology is been used by an attacker to make data recovery more difficult task for the forensic investigator.

B. ***Disabling the log creating system software***- Disabling tool called as Event manager which is responsible for creation of source such as modified windows registry, logon user, computer setting, application software installation etc.

C. ***Live CDs and Virtual Disks***-

Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

D. ***Bootable USB tokens*** **-** These are similar to a Live CD except that the operating system is contained within an attachable USB device. These tokens can typically store more information thanCDs and allow information to be saved, generally via encryption.

[70]Metasploit LLC. (2007a). Metasploit Anti-forensics home page. Retrieved September 11, 2007, from <http://www.metasploit.com/projects/antiforensics/>

E. ***Virtual Machine*****-** These are the "client" operating systems run inside a virtualization program such as VMWare Player, Parallels, or Microsoft Virtual PC.

F. ***Cloud Storage*** **-**In this method fraudster creates the anonymous account with different email service providers and keep the data on their cloud service which is entirely different computers. An attacker may also use some cloud services for launching an attack.

G. Live CDs are an operating system distribution that boots and runs from a read-only device. Live CDs typically have a window system, web browser and SSH client, and run with virtual memory disabled.

HIDING EVIDENCE

It mainly addresses the methods by which the data can be hidden inside the device or over transit. It makes cyber examination process more difficult. The more hurdles have been created when multiple data hiding techniques are clubbed together.[71]

A. ***Encryption*****-** Encryption techniques transparently encrypt data when it is written to the disk and decrypt data when it is read back.
B. ***Steganography*****-**Steganography can be used to embed encrypted data in a cover text to avoid detection. This technique mainly used to embeds text in JPEG, MBP, MP3, WAV and other multimedia files.
C. ***Slack space*****-**Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current generation of forensic tools.
D. Data can also be hidden in unallocated or otherwise unreachable locations that are ignored by the current
E. Generation of forensic tools

[71] Palmer, G (2001, November 6) A Road Map for Digital Forensics Research. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final. Retrieved September 11, 2007, from <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

F. ***HPA*** **-**Information can be stored in the Host Protected Area (HPA) and the Device Configuration Overlay (DCO) areas of modern ATA hard drives. Data in the HPA and DCO is not visible to the BIOS or operating system, although it can be extracted with special tools.

G. ***Program packers*** **-** Packers are commonly used by attackers so that attack tools will not be subject to reverse engineering or detection by scanning.

H. ***Onion Routing*** **-** It combines both approaches with multiple layers of encryption so that no intermediary knows both ends of the communication and the plaintext content.

DESTROYING EVIDENCE

This technique is used to make the evidence useless or unavailable. Evidence can be partly or completely destroyed.

A) ***Bad Sector-*** Attacker intentionally converts good sectors into bad sectors to make data recovery difficult in this scenario.

B) ***Disk degaussing-*** It is a process by which a magnetic field is applied to a digital media device. This may partially or permanently wipe the data within the disk.

COUNTERFEITING EVIDENCE

If computer criminal can found digital evidence he can create inconsistency in data retrieval, it will not credible enough to be presented in a court. Examples of this are timestamp modification and hash collision. Hence counterfeiting can be used to create fake evidence to mislead the forensic investigator.

a) OVERWRITING DATA

Overwriting programs typically operate in one of three modes:

- The program can overwrite the entire media.
- The program can attempt to overwrite individual files. This task is complicated by journaling file systems. The file itself may be overwritten, but portions may be left in the journal.
- The program can attempt to overwrite files that were previously “deleted” but left on the drive.

b) OVERWRITING METADATA

Meta Data is the extra relevant data created by files which may contain vital information. For example, it is frequently possible to determine which files the attacker accessed, by examining file "access" times for every file on the system. Metadata over wiring can confuse the investigator regarding the timeline analysis of the evidence.

c) ARTEFACT WIPING

The methods used in artefact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities.

1.11 CONCLUSION

Sometimes, the process of deleting the evidence itself also create other evidence. Hence it's up to the persistent effort of the forensic investigator. Attacker sometimes ends up creating more traces while trying to use these anti-forensics techniques. Investigation of such expert criminals is very much possible. The golden rule here is not a single crime is full proof. The mistake is the part of human behaviour and criminals are no exception to this. Hence even though there are such techniques available forensics investigation achieve its goal and reveals the facts.

1.12 LET'S SUM UP

In this chapter, we have studied the meaning of digital evidence and the difference between physical and digital evidence. We also studied the detailed procedure of seizure proceedings by Investigation officer. Finally, we ended our discussion with the primary goals of anti-forensics and the different types of anti-forensics.

1.13 FURTHER READING

- https://www.academia.edu/26177741/Computer_Anti-forensics_Methods_and_Their_Impact_on_Computer_Forensic_Investigation
- Beer, Richard &Stander, Adrie& Van Belle, Jean-Paul. (2014). Anti-Forensic Tool Use and Their Impact on Digital Forensic Investigations: A South African Perspective.
- Conlan, Kevin &Baggili, Ibrahim &Breitinger, Frank. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation. 18. 10.1016/j.diin.2016.04.006.

- R. Harris, “Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem,” Digital Investigation, vol. 3, pp. 44-49, 2006.
- C. S. J. Peron and M. Legary, “Digital anti-forensics: emerging trends in data transformation techniques,” in Proceedings of E-crime and Computer Evidence Conference, Technip, Monaco, 2005.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is digital evidence?

Digital evidence or electronic evidence is “any probative information stored or transmitted in digital form that a party to a court case may use at trial”.

2. What are the 2 sources of digital evidence?

- Volatile Evidence
- Non-Volatile Evidence

3. What is anti-forensics?

Anti-forensic is a method used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.

4. What are the primary goals of anti-forensics?

- Avoiding detection of the traces created by a certain incident.
- To make it hard or impossible to retrieve information.
- Increase the time of forensic examination.
- Casting doubt on a forensic report or testimony.
- Misguide the forensic investigator by producing false results.
- Intentional destruction of possible evidence.
- Create inaccuracy in forensic findings.

1.15 ACTIVITY

Explain the different types of anti-forensic techniques along with a case study in which one of the technique is used? (1000 words)

Unit 4: Network Investigations

4

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Overview of enterprise networks

1.4 Overview of Protocols

1.5 Evidence preservation on networks

1.6 Collecting and interpreting network device configuration

1.7 Virtual Private Networks

1.8 Forensic Examination of Network Traffic

1.9 Intrusion detection systems

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of enterprise networks and protocols
- Collecting and interpreting network device configuration
- Forensic examination of network traffic

1.2 INTRODUCTION

Tracking down computer criminals generally requires digital investigators to follow the cybertrail between the crime scene and the offender's computer. The cybertrail can cross

multiple networks and geographical boundaries, and can be comprised of many different kinds of digital evidence, including proxy and firewall logs, intrusion detection systems, and captured network traffic. Dialup server logs at the suspect's Internet Service Provider (ISP) may show that a specific IP address was assigned to the suspect's user account at the time. The ISP may also have Automatic Number Identification (ANI) logs—effectively Caller-ID—connecting the suspect's home telephone number to the dialup activity. Routers on the ISP network that connect the suspect's computer to the Internet may have associated NetFlow logs containing additional information about the network activities under investigation. Each of these logs would represent steps on the trail.[72]

Ideally, each step in the cybertrail can be reconstructed from one or more records from this evidence, enabling digital investigators to connect the dots between the crime scene and the offender's computer and establish the continuity of offense. If there is more than one type of evidence for a particular step, so much the better for correlation and corroboration purposes. Your reconstruction of events is like a scientific hypothesis. The more evidence you collect that is consistent with the hypothesis, the stronger the case for that hypothesis becomes.

Networks present investigators with a number of challenges. When the networks are involved in a crime, evidence is often distributed on many computers making a collection of all hardware or even the entire contents of a network unfeasible.

1.3 OVERVIEW OF ENTERPRISE NETWORKS

Digital investigators must be sufficiently familiar with network components found in a typical organization to identify, preserve, and interpret the key sources of digital evidence in an Enterprise. This chapter concentrates on digital evidence associated with routers, firewalls, authentication servers, network sniffers, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS).

Logs generated by network security devices like firewalls and IDSs can be a valuable source of data in a network investigation. Access attempts blocked by a firewall or malicious activities

[72]Spiekermann, Daniel &Eggendorfer, Tobias (2017) Challenges of Network Forensic Investigation in Virtual Networks. Journal of Cyber Security and Mobility

detected by an IDS may be the first indication of a problem, alarming system administrators enough to report the activity to digital investigators.Routers form the core of any large network, directing packets to their destinations. Routers can be configured to log summary information about every network connection that passes through them, providing a bird's eye view of activities on a network. For example, suppose you find a keylogger on a Windows server, and you can determine when the program was installed. Examining the NetFlow logs relating to the compromised server for the time of interest can reveal the remote IP address used to download the keylogger. Furthermore, NetFlow logs could be searched for that remote IP address to determine which other systems in the Enterprise were accessed and may also contain the keylogger. As more organizations and ISPs collect NetFlowrecords from internal routers as well as those at their Internet borders, digital investigators will find it easier to reconstruct what occurred in a particular case.

Digital investigators may be able to obtain full network traffic captures, which are sometimes referred to as logging or packet capture, but are less like a log of activities than like a complete videotape of them—recorded network traffic islive, complete, and compelling. Replaying an individual's online activities as recorded in a full packet capture can give an otherwise intangible sequence of events a very tangible feel.[73]

1.4 OVERVIEW OF PROTOCOLS

To communicate on a network, computers must use the same protocol. For example, TCP/IP is the standard for computers to communicate across the Internet. The principle is fairly straightforward. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination.[74] This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer. One layer, for instance, is

[73]Spiekermann, Daniel & Keller, Jörg&Eggendorfer, Tobias(2017) Network forensic investigation in OpenFlow networks with ForCon. Digital Investigation

[74] Stevens, S W (1994) In TCP/IP Illustrated, Volume 1: The Protocols. Addison Wesley

used to specify the IP address of the destination system, and another layer is used to specify the destination application on that system by specifying the port being used by that application (there may be several ports on a server willing to receive data, and you don't want your request for a web page to end up in an SSH server). Bothof these layers will contain instructions for reconstructing the separated chunks, how to deal with delayed or out-of-order deliveries, and so forth.

To communicate with machines on different networks, computers must run higher-level protocols such as Internet Protocol (IP) at the network layer and Transport Control Protocol (TCP) at the transport layer.The Transmission Control Protocol (TCP) is a connection-mode service, often called a virtual-circuit service that enables transmission in a reliable, sequenced manner that is analogous to a telephone call. TCP differs from the User Datagram Protocol (UDP), which is connectionless, meaning that each datagram is treated as a self-contained unit rather than part of continuous transmission, anddelivery of each unit is not guaranteed—analogous to a postal letter. Both TCP and UDP use ports to keep track of the communication session.[75]

1.5 EVIDENCE PRESERVATION ON NETWORKS

There are some unique forensic challenges associated with preserving digital evidence on networks. Although some network-related data are stored on hard drives, more information is stored in the volatile memory of network devices for a short time or in-network cables for an instant. Even when collecting relatively static information such as firewall log files, it may not be feasible to shut down the system that contains these logs and then make a bitstream copy of the hard drive. The system may be a part of an organization's critical infrastructure and removing it from the network may cause more disruption or loss than the crime. Alternately, the storage capacity of the system may be prohibitively large to copy. So, how can evidence on a network be collected and documented in a way that demonstrates its authenticity, preserves its integrity and maintains the chain of custody?

[75] Davie, B and Gross, J (2016)A Stateless Transport Tunneling Protocol for Network Virtualization. Internet Draft, Informational: New York, NY

In the case of log files, it is relatively straightforward to make copies of the files, calculate their message digest values (or digitally sign them), and document their characteristics (e.g., name, location, size, MAC times). All this information can be useful for establishing the integrity of the data at a later date and digitally signing files is a good method of establishing chain of custody, provided only a few people have access to the signing key. A failure to take these basic precautions can compromise an investigation. In 2000, for example, an individual known as Maxus stole credit card numbers from the Internet retailer CD Universe and demanded a $100,000 ransom. When denied the money, he posted 25,000numbers on a web site. Employees from one or more of the computer security companies that handled the break-in inadvertently altered log files from the day of the attack—this failure to preserve the digital evidence eliminated the possibility of a prosecution.[76]

Networked systems can also contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the computer is turned off. For instance, active network connections can be used to determine the IP address of an attacker. Methods and tools for preserving volatile data on Windows and UNIX systems are covered in Malware Forensics.

In addition to preserving the integrity of digital evidence, it is advisable to seek and collect corroborating information from multiple, independent sources. Last but not least, when collecting evidence from a network, it is important to keep an inventory of all the evidence with as much information describing the evidence as possible (e.g., filenames, origin, creation times/dates, modification times/dates, a summary of contents). Although time-consuming, this process facilitates the pin-pointing of important items in the large volume of data common to investigations involving networks.

1.6 COLLECTING AND INTERPRETING NETWORK DEVICE CONFIGURATION

Network devices are generally configured with minimal internal logging to conserve storage space and for optimal performance. Some network device functions are so thoroughly engineered to optimize performance that they are not normally logged at all. Although these devices can be

[76]MosharafKabirChowdhury, N M, and Boutaba, R (2009) Network virtualization: state of the art and research challenges. IEEE Commun. Mag. 47, 20–26

configured to generate records of various kinds, the logs must be sent to a remote server for safekeeping because these devices do not contain permanent storage. Central syslog servers are commonly used to collect the log data.

In addition to generating useful logs, network devices can contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the device is shut down or rebooted. Routers are a prime example of this. Most routers are specialized devices with a CPU; ROM containing power-on self-test and bootstrap code; flash memory containing the operating system; nonvolatile RAM containing configuration information; and volatile RAM containing the routing tables, ARP cache, limited log information, and buffered packets when traffic is heavy.[77]

Routers are responsible for directing packets through a network to their destination and can be configured using Access Control Lists (ACLs) to make basicsecurity-related decisions, blocking or allowing packets based on simple criteria. For instance, some organizations implement simple egress and ingress filtering in their border routers (blocking outgoing packets that have source addresses other than their own, and blocking incoming packets that contain source addresses belonging to them). This simple concept—only data addressed from the organization should be allowed out—greatly limits a malicious individual's ability to conceal his location. In some cases, digital investigators must document how a router is configured and other data stored in memory.

1.7 VIRTUAL PRIVATE NETWORKS

Many organizations use Virtual Private Networks (VPN) to allow authorized individuals to connect securely to restricted network resources from a remote location using the public Internet infrastructure. For instance, an organization might use a VPN to enable travelling sales representatives to connect to financial systems that are not generally available from the Internet. Using a VPN, sales representatives could dial into the Internet as usual (using low cost, commodity Internet service providers) and then establish a secure, encrypted connection the

[77] Corey, V, Peterman, C, Shearin, S., Greenberg, M S, and Van Bokkelen, J (2002) Network forensics analysis. IEEE Int. Comput. 6, 60–66

organization's network. A VPN essentially provides an encrypted tunnel through the public Internet, protecting all data that travels between the organization's network and the sales representative's computer.

Newer operating systems, including Windows 2000/XP/Vista, have integrated VPN capabilities, implementing protocols like Point to Point TunnelingProtocol (PPTP) and IPsec to establish VPN. Newer network security devices like the Cisco ASA and Juniper SA Series also support VPN services via SSL, enabling users to establish a virtual connection simply using a web browser.Digital investigators most commonly encounter VPN logs as a source of evidence associated with remote users accessing secured resources within the network from the Internet.

1.8 FORENSIC EXAMINATION OF NETWORK TRAFFIC

The contents of network traffic can be invaluable in a network investigation, because some evidence exists only inside packet captures. Many host-based applications do not keep detailed records of network transmissions, and so capturing network traffic may provide you with information that is not recorded on a host. Furthermore, captured network traffic can contain full packet contents, whereas devices like firewalls and routers will not. Even an IDS, which may record some packet contents, typically only does so for packets thatspecifically trigger a rule, whereas a sniffer can be used to capture all traffic based upon the requirements of the investigator.[78]

Extracting Statistical Information From Network Traffic

Whether you are approaching network traffic without any leads or you have some items like IP addresses that you can use to filter or search, you should examine the set of packets in a methodical manner to extract data of interest for your investigation.[79] Examples of data you might want to extract include:

- Statistics
- Alert data

[78] Hunt, R, and Zeadally, S (2012) Network forensics: an analysis of techniques, tools, and trends. IEEE Comput. 45, 36–43

[79]Jain, R, and Paul, S (2013). Network virtualization and software defined networking for cloud computing: a survey. IEEE Commun. Mag. 51, 24–31

- Web pages
- E-mails
- Chat records
- Files being transferred
- Voice conversations

Extracting Statistics

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

1.9 INTRUSION DETECTION SYSTEMS

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS). Some of these systems such as Bro (www.bro-ids.org) can be configured to store all traffic and then examine it for known attacks and to archive significant features of network traffic for later analysis. Other systems such as Snort (www.snort.org) inspect the traffic and store only data that appear to be suspicious, ignoring anything that appears to be acceptable. These systems are not primarily concerned with preserving the authenticityand integrity of the data they collect, so additional measures must be taken when using these tools.[80]

Although they are not designed specifically for gathering evidence, logs from an IDS can be useful in the instance of an offender breaking into a computer. Criminals who break into computers often destroy evidence contained in log files on the compromised machine to make an investigator's job more difficult. However, an IDS keeps a log of attacks at the network level that investigators can use to determine the offender's IP address. For example, if fraud is committed

[80]Delgadillo, K (2015)Netflow services and applications. Cisco Whitepaper, 1996 (accessed November 5, 2015)

using a networked computer and investigators find that the computer was compromised and then scrubbed of all evidence, they may be able to determine which IP address was used by examining the log file from an IDS on the network.

While investigating a large-scale network intrusion, network traffic showed the intruder connecting to a compromised system and placing an unknown executable on the system via SMB. A subsequent forensic examination of the compromised computer revealed that the intruder had deleted the unknown executable and it could not be recovered from thehard drive. Although available tools for examining network traffic could not extract the file automatically, we were able to recover the unknown executable manually and examine it to determine its functionality. The information obtained from this executable helped advance the investigation in a variety of ways.

For example, A financial services company offered customers personalized web service to monitor their financial information, including credit ratings. Each customer had an account that could be verified for two levels of access, Tier 1 and Tier 2. The Tier 1 authentication would allow a customer to view commercially available information collected at the site. To view or to makechanges to their financial data, they needed a Tier 2 authentication, which required a different password and answers to some challenge questions.[81]

Web administrators would authenticate to both servers as well, but at Tier 2 their accounts had administrative access tothe web site and its databases and thus to everyone's financial information.During routine maintenance, several fixes to minor problems were implemented simultaneously. As a result of the interactions of these fixes, every account on the system had full administrative access to all the accounts at Tier 2.

The problem went undetected for several months until reported by one of the customers. The administrative accesswas not obvious and could be discovered only by trying to access someone else's financial information. It would not occur to most customers to try the experiment. Since it was one of the customers who discovered the problem, though, it obviously could happen.Forensic investigators were asked to analyze available logs covering the vulnerable

[81] Khan, S, Gani, A, Abdul Wahab, A W, Shiraz, M, and Ahmad, I (2015) Network forensics: review, taxonomy, and open challenges JNetwComputAppl 66, 214–235

period to determine whether it was likely that any customers had exploited the information of others.

1.10 LET' S SUM UP

In order to conduct an investigation involving computer networks, practitioners need to understand network architecture, be familiar with network devices and protocols, and have the ability to interpret the various network-level logs. Practitioners must also be able to search and combine large volumes of log data using search tools like Splunk or custom scripts. Perhaps most importantly, digital forensic analysts must be able to slice and dice network traffic using a variety of tools to extract the maximum information out of this valuable source of network-related digital evidence.

1.11 FURTHER READING

- Bunker, M., & Sullivan, B. (2000). CD Universe Evidence Compromised. MSNBC, June 7.
- Comer, D. E. (1995). Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture (Third Edition). Upper Saddle River, NJ: Prentice Hall.
- Villano, M. (2001). Computer Forensics: IT Autopsy, CIO Magazine, March (http://www.cio.com/article/30022/Computer_Forensics_IT_Autopsy).
- Plonka, D. (2000). FlowScan: A Network Traffic Flow Reporting and Visualization Tool. Usenix.
- Casey, E. (2004a). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What are Intrusion Detection Systems?

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS).

2) Short note on protocols?

To communicate on a network, computers must use the same protocol. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination. This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer.

3) How to generate statistics from a set of network traffic?

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

1.13 ACTIVITY

Explain briefly about Network investigations along with how networks are used in the forensic examination? Write a relevant case study pertaining to network traffic and examination? (800-1000 words)

Block 3
Role and Analysis of Cyber Forensics

Unit 1: Computer Forensics and Its Significance

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Relevance of Cyber Forensics

1.4 The Concept of Cyber Forensics

1.5 Various Tools of Cyber Forensics

1.6 Conclusion

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The relevance of cyber forensics
- The concept of cyber forensics
- The various tools used in the implementation of cyber forensics

1.2 INTRODUCTION

The concept of cyber forensics is relatively new in India. The advent of high-speed broadband and mobile internet network at affordable rates has made internet highly accessible to people. However, the improving infrastructure has also contributed to a rise in cyber crimes in India.[82]Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

1.3 RELEVANCE OF CYBER FORENSICS

In the case of traditional crimes, the investigating agency visits the crimes scene and collects evidence through various means such as collecting various objects of interest from the crime scene, interacting with the witnesses to the crime, etc. Thus, there is a sense of tangibility to a crime which takes place in the physical world.

However, in the case of cyber crime, the said act is devoid of the same sense of physicality. Since a cybercrime takes place using a computer or such other devices from a remote location, the methods used to detect a traditional crime cannot be employed. One must also remember that since a majority of people are not as well versed with cyberspace, i.e. the notional environment in which communication over computer networks take place, detecting cyber crimes is way more difficult than that of traditional crimes.

Using cyber forensics, the investigating agency is able to gather the evidence pertaining to the commission of cybercrime, including the identity of the perpetrator. The chief objective of cyber forensics is to obtain evidence using various techniques which can be used to make a case before the court of law. A number of cyber crimes such as phishing, hacking, fraud, cyber espionage, cyber terrorism are investigated with the help of cyber forensics. It can be said that without employing the necessary measures afforded by cyber forensics, a number of crimes would have remained unproved and inconclusive.[83]

An important example of the effectiveness of cyber forensics is the BTK serial killer case. From 1974 to 1991 a number of murders took place in Kansas, the United States of America which

[82]Armstrong, I (2002) Computer Forensics Detecting the Imprint. SC Magazine
[83]Sadiku, Matthew &Tembely, Mahamadou& Musa, Sarhan.(2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

were suspected to have been committed by a serial killer. However, the investigating authorities were unable to find the culprit behind the killings. In 2004, the investigating agencies started receiving a number of communications from the perpetrator. Some of these communications were sent on a floppy drive. On examination of the floppy disk by cyber forensic experts, it was found that a Microsoft Word document had been deleted from the floppy drive. By analysing the metadata related to the Word document, the investigating agency were able to determine the identity of the perpetrator and the said evidence was considered by the courts while finding Dennis Rader guilty of committing the murders.

1.4 THE CONCEPT OF CYBER FORENSICS

In order to connect to the cyberspace, a user requires to connect to the internet through an Internet Service Provider (ISP). In order to connect to the internet, a user utilises a dial up connection / broadband connection or a mobile network.[84] Thus, in order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

Computers maintain data related to the files used by the user in the form of logs. Even if the data is deleted, the logs related to such data is stored in the hard drive through swap files, memory dumps and other unallocated spaces in the hard drive.

Further, when accessing websites, the information is cached in the machine accessing the website. The Oxford Learners Dictionary defines a "cache" as a part of computer's memory that stores copies of data that is often needed while a program is running. "Caching" stores the data related to the web page on the hard drive of the computer.

ISPs maintain logs of the websites visited by users availing internet services through its portals including the IP address and machine ID (Mac ID) of the user.

Using various techniques of cyber forensics, an investigation agency can gather evidence to prove that a machine has been used by the user to commit a cyber crime.

[84]Mandia, Prosise, Pepe Incident Response & Computer Forensics Second Edition. McGraw-Hill 2003

1.5 VARIOUS TOOLS OF CYBER FORENSICS

Before dealing with the various techniques of cyber forensics, it is pertinent to discuss the legal framework.[85]

Section 76 in The Information Technology Act, 2000 ("**IT Act**") deals with confiscation of data.[86]

> ***76. Confiscation***.-*Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:*
>
> *Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.*

Further Section 77A of the IT Act provides for compounding of offences committed under the IT Act.

> ***77A. Compounding of Offences****- (1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.*

[85]US Department of Justice Computer Crime and Intellectual Property Section, Criminal Division. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002 NIJ Electronic Crime Scene Investigation – A Guide for First Responders 2001. NHTCU Good Practice Guide for Computer Based Electronic Evidence 2003

[86]IT Act: Offences (Section 65 to 78)
<https://informationtechnologyactindia.blogspot.com/p/offences-section-65-to.html>

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section 265B, Code of Criminal Procedure, 1973

265B. Application for plea bargaining *-A person accused of an offence may file an application for plea bargaining in the Court in which such offence is pending for trial.*

The application under Sub-Section (1) shall contain a brief description of the case relating to which the application is filed including the offence to which the case relates and shall be accompanied by an affidavit sworn by the accused stating therein that he has voluntarily preferred, after understanding the nature and extent of punishment provided under the law for the offence, the plea bargaining in his case and that he has not previously been convicted by a Court in a case in which he had been charged with the same offence.

After receiving the application under Sub-Section (1), the Court shall issue a notice to the Public Prosecutor or the complainant of the case, as the case may be, and to the accused to appear on the date fixed for the case.

When the Public Prosecutor or the complainant of the case, as the case may be, and the accused appear on the date fixed under Sub-Section (3), the Court shall examine the accused in camera, where the other party in the case shall not be present, to satisfy itself that the accused has filed the application voluntarily and where-

the Court is satisfied that the application has been filed by the accused voluntarily, it shall provide time to the Public Prosecutor or the complainant of the case, as the case

may be, and the accused to work out a mutually satisfactory disposition of the case which may include giving to the victim by the accused the compensation and other expenses during the case and thereafter fix the date for further hearing of the case;

the Court finds that the application has been filed involuntarily by the accused or he has previously been convicted by a Court in a case in which he had been charged with the same offence; it shall proceed further in accordance with the provisions of this Code from the stage such application has been filed under Sub-Section (1).

Section 265C of Criminal Procedure Code, 1973

S. 265C Guidelines for mutually satisfactory disposition In working out a mutually satisfactory disposition under clause (a) of Sub-Section (4) of section 265B, the Court shall follow the following procedure, namely;

in a case instituted on a police report, the Court shall issue a notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case;

Provided that throughout such process of working out a satisfactory disposition of the case, it shall be the duty of the Court to ensure that the entire process is completed voluntarily by the parties participating in the meeting;

Provided further that the accused may, if he so desires, participate in such meeting with his pleader, if any, engaged in the case;

in a case instituted otherwise than on police report, the Court shall issue a notice to the accused and the victim of the case to participate in a meeting to work out a satisfactory disposition of the case;

Provided that it shall be the duty of the Court to ensure, throughout such process of working out a satisfactory disposition of the case, that it is completed voluntarily by the parties participating in the meeting;

Provided further that if the victim of the case or the accused, as the case may be, so desires, he may participate in such meeting with his pleader engaged in the case.

To give effect to the content addressed through such aforementioned provisions of the legal framework in the country, there are various techniques implemented that act as tools. Such tools are majorly used for collecting digital evidence related to various limbs of cyberlaw such as disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

Disk Forensics Tool aims at addressing concerns arising in association with data recovery, data analysis, tracking senders of emails, analysing forensic registry, extracting forensic thumbnail, etc.

Network Forensics Tool aims at addressing concerns arising in association with analysis of forensic log, tracing sender of emails, analysing network sessions, etc.

Mobile Device Forensics Tool aims at addressing concerns arising in association with the acquisition of software, analysis of mobile phones and smartphones, analysis of mobile devices, analysis of call data records of various service providers, creation of forensic solution for imaging, analysis of sim cards, etc.[87]

Live Forensics Tool aims at addressing concerns arising in association with arriving at software solutions related to acquisition and analysis of volatile data in systems.

Tools of cyber forensics are used and implemented to extract digital evidence that can be used and admitted in courts of law. Since electronic evidence plays a vital and pivotal role in cybercrimes, tools of cyber forensics act as the basis of digital media by allowing anti-forensic techniques to be countered.

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect. These two machines communicate with each other using a serial. The DESK system searches for and identifies the keywords in Chinese and/or English using a text pattern file, to locate the words searched for on the subject machine. The DESK function

[87] Bynum, T. (2001) Computer Ethics: Basic Concepts and Historical Overview Stanford Encyclopedia of Philosophy Retrieved 12 January 2007 from
<http:// plato.stanford.edu/archives/win2001/entries/ethics-computer/>

further uses the hash value database that contains fingerprints of certain systems of the file so as to enable verification of file integrity.

The DESK function involves three types of searches:

a Physical Search – This involves performing a search of patterns of individual physicalsectors in the storage of the subject machine. Owing to such physical search, evidence of cybercrime stored in unused sectors can be discovered with ease. It further allows locating files independent of the specific file systems.

b Logical Search – This kind of search involves making use of information regarding the file system concerned. A file, which is conceptually a sequence of bytes, is placed in portions of the sequence into different sectors by the file system, in accordance with the logical continuity of the contents thereof.

c Deleted File Search – File deletion, in most file systems, is accomplished by way of modifying only a few bytes of the file system, thereby allowing the content of a deleted file to subsist in the storage system, unless overwritten. Therefore, patterns in deleted files can be traced back until the time that the disk sectors are overwritten by other new files.

1.6 CONCLUSION

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to go it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favor.

1.7 LET'S SUM UP

In this chapter, we studied the significance of computer forensics and its relevancy. We discussed the concept of cyber forensics and finally, ended the discussion with various tools used in cyber forensics and provisions pertaining to it under the Information Technology Act.

1.8 FURTHER READING

- Bell, G., and Boddington, R. (2010). Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? The Journal of Digital Forensics, Security and Law, Vol 5(3).
- De Forest, P. R., Gaensslen, R. E., and Lee, H. C. (1983). Forensic Science: An Introduction to Criminalistics, McGraw-Hill, New York.
- Menn, J. (2010). Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, PublicAffairs, New York.
- Gogolin, G. (2010). The Digital Crime Tsunami. Digital Investigation, Vol. 7(1-2).
- Kind, S., and Overman, M. (1972). Science against Crime, Aldus Books, London, UK

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of cyber forensic?

Cyber forensic is the tool which is employed to detect cybercrimes and to prevent cybercrimes before the crime is committed.

2) What are the methods/sources that need to be used to obtain evidence in cyber forensic?

In order to obtain evidence, an investigation agency can gather evidence from the following sources:

- The user's computer;
- The servers of the ISP used by the user

3) What is the most important tool in cyber forensic?

The most useful tool used in cyber forensics is the Digital Evidence Search Kit (DESK), which is a machine that law enforcement agents; it further involves the use of a subject machine, which is the device used by the suspect.

4) What are the 3 types of searches under desk function?

The DESK function involves three types of searches:

a Physical Search

b Logical Search

c Deleted File Search

1.10 ACTIVITY

Explain the concept and relevancy of cyber forensics in the present era, along with the various tools that are used to gather evidence and relevant provisions under the I.T. Act? (800-1000 words)

Unit 2: Windows Forensics Analysis 2

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Windows XP
1.4 Windows Vista (and related systems)
1.5 Overview of NTFS
1.6 Data Access Control
1.7 Forensic Analysis of the NTFS Master File Table (MFT)
1.8 NTFS File Deletion
1.9 Let's sum up
1.10 Further reading
1.11 Check your progress: Possible answers
1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The process of Windows XP, Vista etc under forensics
- Forensic analysis of the NTFS Master file table
- Data access control and file deletion

1.2 INTRODUCTION

Despite the proliferation and growing popularity of other user interfaces, such as Macintosh OS X and Ubuntu (a flavor of Linux), Microsoft's Windows operating systems remain the most popular in the world. Sources have reported that over 90% of the computers in use today are running some version of the Windows operating system.1 This is not surprising given the almost endless variation that can be found in Windows products, their relative ease of use for the average computer owner, and the virtual stranglehold on marketing Microsoft has enjoyed for so many years (particularly before recent inroads by a resurgent Apple, Inc.). Microsoft operating systems have even found an audience in non-traditional quarters, as scores of Macintosh users have learned to use products like Apple's Boot Camp or Parallels virtualization software to run Windows on their Intel-based Macintosh hardware. Private users, Fortune 500 companies, and government agencies alike all overwhelmingly have chosen Windows systems as their primary technology infrastructures.[88]

In light of this, it should not be surprising that the majority of systemsthat digital investigators will be called upon to examine will be running a Windows operating system. The ease of use of Windows appeals to criminals and "evil-doers" the same as it does to the grandmother downthe street. And both the longevity and popularity of Windows have made it a favorite target of virus authors, hackers, and industrial saboteurs. So, whether investigating child pornography, intellectual property theft, or Internet Relay Chat (IRC) botinfection, it is a safe bet that knowledge of Windows operating systems, and its associated artifacts, will aid investigators in their task.

1.3 WINDOWS XP

Windows XP has been a standard Microsoft OS for workstations for years. Since it hit the scene in 2001, millions of Windows users have grown comfortable with its user-friendly interface,

[88] Brill, A (2006b) The Brill files: An investigative report on data wiping utilities—Part two. Kroll Ontrack Newsletter, 4(6). Available online at <www.krollontrack.com/ newsletters/cccfn_0606.html>

comparatively efficient operation, and improvements over previous versions such as Windows 2000 and Windows ME. Windows XP comes in three primary editions (i.e., Home, Media Center, and Professional), which were targeted at different parts of Microsoft's work-station computing customers. From a file system standpoint, XP continues to run on top of the File Allocation Table (FAT) and New Technology File System (NTFS) structures with which examiners have grown familiar.[89]

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool. However, other challenges (such as analyzing restore points, analysis of data in the Windows registry, collection and analysis of memory, dealing with RAIDs and dynamic disks, overcoming Windows encryption, and documenting data destruction) can present a much greater challenge, even for more experienced digital investigators. Regardless of its utility, Microsoft stopped selling XP in 2008 but plans to continue support for this beloved Windows version until 2014, which means it will most likely be a big part of examiners' lives for many years to come.[90]

1.4 WINDOWS VISTA (AND RELATED SYSTEMS)

Windows Vista, which many still remember under its development code name of "Longhorn," was officially released in 2007 and, like XP before it, was intended by Microsoft to become the de facto OS for workstations. Vista, like XP (and the upcoming Windows 7), is available in multiple editions(i.e., Starter, Home Basic and Basic N, Home Premium, Business and Business N, Enterprise, and Ultimate), each with its capabilities and features; for example, Vista Home allows users to back up documents, and Vista Enterprise allows the creation of true-clone copies of the entire hard disk/partitions for later recovery or creation of identical systems.[91]

[89] Geiger, M (2005). Evaluating commercial counter-forensic software.In Proceedings of DFRWS 2005. Available online at <www.dfrws.org/2005/proceedings/geiger_ counterforensics_slides.pdf>

[90]Grand, J, & Carrier, B (2004) A hardware-based memory acquisition procedure for digital investigations.Journal of Digital Investigation, 1(1), 1742–2876. Available online at <www.digitalevidence.org/papers/tribble-preprint.pdf>

[91]Hargreaves, C, Chivers, H, &Titheridge, D (2008) Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48

Also similar to XP, Vista, 2k8, and 7 take advantage of the NTFS file system and add the concept of Transactional NTFS (TxF). Implemented together with the Kernel Transaction Manager (KTM), TxFwas designed to make NTFS more robust by treating file operations as transactions that can be rolled back or reapplied as necessary in the case of catastrophic system failure.[92] Most of Microsoft's official literature suggests that Vista cannot be installed and run on FAT32. However, although this may be true from a simplistic or tech support stand-point, there are several tips and tweaks that will allow Vista to be installed on a FAT32 partition, so it is possible the digital investigator could encounter such a scenario. Before Vista was released, it was thought it would be based on a new file system (WinFS) under development by Microsoft. However, shortly before Vista's release, problems in development caused Microsoft to shelve the new file system temporarily, leaving Vista to utilize NTFS as its primary base.

1.5 OVERVIEW OF NTFS

While the world waits for WinFS, most modern Windows workstations and servers are using the much more familiar NTFS. NTFS is an alternative to FAT file systems (e.g., FAT12, FAT16, FAT32) and can be utilized by Windows NT/2k/XP/2k3/Vista/2k8 operating systems. The current version is NTFS 3.1, which has been used in Windows XP and later OS releases. Among improvements in NTFS file systems are increased file size potential (roughly 16TB versus 4GB for FAT32), increased volume size potential (roughly 256TB versus 2TB for FAT32), and the recording of Last Accessed times (in Windows NT/2k/XP/2k3, and Vista/2k8/7 if enabled). In addition, NTFS uses a data structure called the Master File Table (MFT) and entries called index attributes instead of a file allocation table (FAT) and folder entries in order to make the access and organization of data more efficient. These and other key features of NTFS of interest to forensic examiners are covered in this section.[93]

The primary internal files that NTFS uses to track data sometimes referred to as metadata files. The presence of these internal files on a system being examined (or traces of these files in unallocated space) should indicate to an examiner that the system was formatted as NTFS.It

[92]Kessler, M. (2007).Maintaining Windows 2000 peak performance through defragmentation. Microsoft Technet. Available online at <http://technet.microsoft.com/en-us/library/ bb742585.aspx>

[93]Lee, R (2008) VISTA shadow volume forensics.SANS Computer Forensics and E-Discovery Blog. Available online at <http://sansforensics.wordpress.com/2008/10/10/shadowforensics/>

general, the dates and times associated with these files are set when the files are first created on the volume and do not change over time with the use of the system. As such, the dates and times of these internal files (particularly the Created Date) can be used as an indication of when the volume was last formatted as NTFS. All of these files have their function and can be analyzed to the nth degree, but a few of them can be very useful to the investigator.

In ***Johnson vs Wells Fargo,***[94] a U.S. District Court in Nevada heard a motion on behalf of a defendant alleging that the plaintiff in the case reformatted two hard disk drives possibly containing evidence that the plaintiff falsified documentation to support his claims. The defendant informed the plaintiff of the intent to compel production of the hard disk drives in September 2007; however, the defendant's "forensic computer expert" (the label applied to the defendant's digital investigator in court filings)concluded, upon examination of the system files on the reformatted hard disk drives, that one of the drives was reformatted a mere five days after the plaintiff was notified that he would be compelled to produce it, and the second drive was reformatted only 10 days later. As a result, the Court found that the plaintiff destroyed potential evidence, and a jury instruction adverse to the plaintiff was ordered in the case as a result of his actions.

1.6 DATA ACCESS CONTROL

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders.[95] Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system. This ownership and access information is often quite important to an examiner attempting to determine who had accessto (or who is responsible for) a particular data object. For example, an examiner seeking a clue as to which user account was used to download a particular pornographic picture usually need only look at the picture's owner in NTFS.

[94] *Johnson v Wells Fargo* 635 F 3d 401 (9th Cir) [2011]
[95] Malin, C, Casey, E, &Aquilina, J (2008) Malware forensics Syngress Media

Although these ownership and access values in the $Secure file can be interpreted manually, it is fairly complex and requires data from several different internal NTFS files, so it is far easier for examiners to use a third-party tool.

1.7 FORENSIC ANALYSIS OF THE NTFS MASTER FILE TABLE (MFT)

$MFT RECORD BASICS

Each MFT record has its data structure, to include slack that occurs between the end of the last attribute in the record and the beginning of the subsequent MFT record. Decoding the data in the records can sometimes be tricky, and is normally handled by a forensic tool, but it can be done by hand in the absence of one of these tools or for validation purposes.[96]

In addition to data such as the file status flag described earlier, which resides in each record header (normally the first 56 bytes of the record in XP and later), MFT records are composed of attributes that each have a specific function and structure. Each attribute has its header, which (among other things) identifies the attribute and gives the size of the attribute. It is also useful to understand that these attributes can be resident (meaning, they exist within a given MFT record) or nonresident (meaning, they exist outside a given MFT record, elsewhere on the disk, and are referenced within the record). Among these attributes, the Standard Information Attribute (SIA), Filename Attribute (FNA), and Data Attribute can be most helpful from a forensic perspective.

DATA-TIME STAMP DIFFERENCES BETWEEN NTFS AND FAT

NTFS date-time stamps differ from those recorded on FAT systems in several key ways. First, it is important to note that NTFS and FAT date-time stamps do not reside in the same locations; whereas NTFS uses the $MFT as a primary repository for date and time metadata, FAT systems record dates and times within folder entries. Another major difference is that NTFS date-time stamps are recorded in UTC, regardless of the time zone set for the system, whereas FAT date-time stamps are recorded in local time; this distinction is important, particularly when interpreting the date-time stamps manually. In addition, NTFS represents date-time stamps using the FILETIME format, which represents the number of 100 nanosecond intervals since January

[96] Mueller, L. (2009). Detecting timestamp changing utilities.Professional Blog. Available online at <http://www.forensickb.com/2009/02/detecting-timestamp-changingutlities.html>

1, 1601, and can be interpreted by most forensic tools, including free tools such as DCode by Digital Detective.[97]

The FILETIME format is different from the DOSDATETIME that is primarily used in FAT, which is 4 bytes and starts onJanuary 1, 1980. To confuse matters, on FAT systems the resolution of create time on FAT is 10 milliseconds (additional bytes are used to record hundredths of a second), whereas write time has a resolution of 2 seconds, and access time has a resolution of 1 day, allowing the examiner to be less specific about when a file or folder was last accessed on the file system (Microsoft, 2009a). Even within NTFS, the use of Last Accessed date-stamps can vary. For example, NTFS delays updates to the last access date-time stamps by up to 1 hour after the last access (Microsoft, 2009a).

DATA ATTRIBUTE

An MFT record's Data Attribute can be very important to examiners, chiefly because it contains either the actual data itself (resident) or a pointer to where the data resides on the disk (nonresident). A resident Data Attribute contains the actual data of the file referenced by the MFT record; this occurs when the data the file contains is relatively small in size (usually less than 600 bytes), so small text files (such as boot.ini or Internet cookies) are often held as resident files. For larger files, the MFT contains a list of the clusters allocated to that file, called data runs.

1.8 NTFS FILE DELETION

In the same vein, it is quickly worth mentioning what happens in NTFS when a file is deleted (as opposed to being sent to the Recycle Bin). When a file is deleted in NTFS, many different things happen "under the hood," but among the observable behaviors important to examiners are:

- The deleted file's entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file's parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file to delete it (e.g., right-click on the file).

[97] Park, B, Park, J, & Lee, S. (2008). Data concealment and detection in Microsoft Office 2007 files Journal of Digital Investigation, 5(3–4), 104–114

However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.

- The two bytes located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself is now unallocated and ready for reuse.

A recent investigation focused on a government server, which was found to be beaconing out to another country. The start date of the beaconing traffic gave investigators an approximate date for the compromise of the victim machine, as they began developing their timeline. However, during the forensic examination of the compromised system, the source of the beaconing was found to be a piece of malware (keylogger) whose File Created date-time stamp (as displayed by several different forensic tools) predated the beginning of the beaconing by almost two years.[98] Investigators began to wonderif the system had been compromised much earlier than they originally thought. But, upon more detailed examination of the file's MFT record, and manual translation of the dates and times held in the FNA for the malware and associated files, investigators confirmed that the malware had most likely been created on the system at a date and time that very nearly matched the start of the beaconing traffic, confirming their original timeline. This discovery led to suspicion of SIA date-time stamp alteration on the part of the intruder and the location of a date-time stamp modification utility.

Evidence of file deletion (as opposed to destruction/wiping) by a particular user presents its own set of challenges, particularly since no specific program or utility is required to delete a file in Windows. Simply sending a file to the Recycle Bin is not (by the most common forensic definition) actual deletion of the file; however, a user sending a file to the Recycle Bin is often viewed as legally significant in a case where the user was supposed to be preserving or protecting data. Further, a file in the Recycle Bin is usually easy to identify, and data provided by INFO2 records or $I files (Vista/7 Recycle Bin operation) can help the investigator pinpoint

[98]Parsonage, H (2008).The forensic recovery of instant messages from MSN Messenger and Windows Live Messenger. Available online at
<http://computerforensics.parsonage. co.uk/downloads/MSNandLiveMessengerArtefactsOfConversations.pdf>

where the file was when it was deleted, as well as when the data was sent to the Bin and by which user account. Even if the Recycle Bin is empty, looking at the Last Written date-time stamp on the associated INFO2 record can provide the investigator with valuable data about the approximate time the Recycle Bin was cleared.

Forensic examiners can often recover data and associated metadata for deleted files, even when Recycle Bin information is not available. In particular, when dealing with NTFS, a recovered MFT entry can provide all the information a forensic examiner needs about deleted data. For digital investigators, knowing the mechanics is often a far cry from knowing who deleted the file and when. Most forensic suites have the ability to identify deleted and partially overwritten files, distinguishing them via different icons or information in the files' descriptions.

DETERMINING TIME OF DELETION

A common mistake that forensic examiners can make is to assume that the Last Accessed date-time stamps of deleted files show when the files were deleted. Although it may seem logical in theory that a file would be accessed at the time, it was deleted, this is not always true. For instance, deleting an entire folder does not update the Last Accessed date-time stamp of the files it contains (try it!). As another example, when a user causesInternet Explorer to clear the Temporary Internet Files (e.g., Tools→Delete Browsing History…→Delete Files…, in Internet Explorer 7), it does not update the Last Accessed dates of the files. Without other supporting evidence, the only statement an examiner can safely make about a deleted file based solely on its Last Accessed date-time stamp is that it was not deleted prior to the date indicated by that piece of metadata.[99]

Determining who deleted the file can be even more difficult and often has to be obliquely proven by attempting to correlate system usage data (such as logged on users, etc.) with the last date-time stamps on the deleted file. A determination regarding who deleted a file can also be circumstantially supported by file permissions data (file owner, who has deletion rights, etc.), clues from the location of the deleted file (e.g., c:\Documents and Settings\<username>\My Documents), and link files and MRU registry data that pointed to the data in its active state, but

[99] Mueller, L (2008) Incident response—Recovering a BitLocker recovery password before system shutdown. Professional Blog Available online at <www.forensickb.com/2008/01/ incident-response-recovering-bitlocker.html>

the investigator must correlate and weigh each piece of evidence carefully before opining on the source of a file's deletion.

1.9 LET'S SUM UP

In this chapter, we studied the concept of Windows XP, Vista etc and the process of forensics with respect to it. We also discussed the new technology file system and data access control. Finally, we ended the discussion with forensic analysis of the NTFS MFT and the process of file deletion.

1.10 FURTHER READING

- Carrier, B. (2005). File system forensic analysis. Addison-Wesley.
- Dickson M. (2006). An examination into MSN Messenger 7.5 contact identification. Journal of Digital Investigation, 3(2), 79–83.
- Carvey, H. (2009). Windows forensic analysis (2nd ed.). Syngress Media.
- Geiger, M. (2005). Evaluating commercial counter-forensic software. In Proceedings of DFRWS 2005. Available online at www.dfrws.org/2005/proceedings/geiger_counterforensics_slides.pdf
- Hargreaves, C., Chivers, H., &Titheridge, D. (2008). Windows Vista and digital investigations. Digital Investigation Journal, 5(1–2), 34–48.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) How are the evidence gathered by the examiners in Windows XP?

There are many features in Windows XP that can be very useful for forensic examiners. Evidence of user actions is often recorded in areas (such as Internet history, Event logs, Prefetch files, thumbs.db files, and link files) that are easy to view for the trained digital investigator with the right tool.

2) What is the key feature of NTFS?

One of the key features of NTFS is its increased security over FAT file systems. This security manifests itself in many ways, but perhaps the most noticeable is an access control list (ACL) that governs read-write-execute access to Windows files and folders. Security descriptors stored in the $Secure file, an internal NTFS file that is three data streams, details ownership and access information for files and folders on the file system.

3) What is the process post deletion of files in NTFS?

When a file is deleted in NTFS, many different things happen "under the hood," but among the observable behaviors important to examiners are:

- The deleted file's entry is removed from its parent index, and the file system metadata (i.e., Last Written, Last Accessed, Entry Modified) for the file's parent folder are updated. It is also possible that the metadata for the deleted file itself may be updated because of how the user interacted with the file in order to delete it (e.g., right-click on the file). However, examiners should exercise caution before drawing any conclusions from the metadata of a deleted file without other supporting, or related evidence found elsewhere on the file system.
- The two bytes located at record offset 22 within the file's MFT record are changed from \x01\x00 (allocated file) to \x00\x00 (unallocated file).
- The appropriate locations in $Bitmap are modified to show that both the space occupied by the MFT record and space previously occupied by the file itself sis now unallocated and ready for reuse.

1.12 ACTIVITY

Explain the concept of forensic analysis in Windows XP, Vista and 7 along with the process of deletion of files in NTFS and the process of post deletion? Briefly explain the same with a relevant case study in the present era? (1000 words)

Unit 3: Data Recovery Function Testing For Digital Forensic Tools

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Validation and verification framework

1.4 Data recovery function mapping

1.5 Reasons for data recovery

1.6 Requirements specification

1.7 Recovered Objects

1.8 Reference set development and testing

1.9 Conclusion

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Data recovery function mapping
- Validation and verification framework
- Recovered objects and reference set development and testing

1.2 INTRODUCTION

Many digital forensic tools used by investigators were not originally designed for forensic applications. Even in the case of tools created with the forensic process in mind, there is the issue of assuring their reliability and dependability. Given the nature of investigations and the fact that the data collected and analyzed by the tools must be presented as evidence, it is important that digital forensic tools be validated and verified before they are deployed.Digital forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is acceptable in court-room proceedings.

1.3 VALIDATION AND VERIFICATION FRAMEWORK

Our validation and verification framework is function-oriented and incorporates detailed specifications that are absent in other work. The methodology begins with a systematic description of the digital forensic field using a formal model and function mapping. Digital forensiccomponents and processes are defined in this model , and fundamentalfunctions in the investigative process such as searching, data preservation andfile identification are specified (i.e., mapped). Having developed the model and function mapping, the validation and verification of a digital forensic tool is accomplished by specifying its requirements for each mapped function. Next, a reference set is developed comprising a test case (or scenario) corresponding to each functional requirement. The reference set enables the forensic tool and/or its functions to be validated and verified independently.When a tool is tested, a set of metrics can also be derived to determine the fundamental scientific measurements of accuracy and precision.[100] In summary, if the discipline is mapped in terms of functions (and their specifications) and, for each function, the expected results are identified and mapped as a reference set, then any tool, regardless of its original design intention, can be validated against known elements. The function-oriented validation and verification regime has severaldistinctive features such as detachability, extensibility, tool version neutrality and transparency.

[100] J Beckett and J. Slay, Digital forensics: Validation and verification in a dynamic work environment, Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences, p 266, 2007

1.4 DATA RECOVERY FUNCTION MAPPING

Data recovery is generally regarded as the process of salvaging data partially or completely from damaged, failed, corrupted or inaccessible storage media. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.[101]

A variety of failures can cause physical damage to storage media. CD-ROMs can have their metallic substrate or dye layer scratched off, hard disks can suffer any of several mechanical failures; tapes can break. The logical damage to the data may take the form of corrupt or missing boot-related records (e.g., main boot record, disk partition table and directories) or the loss of file signatures (e.g., header and footer). Since our focus is on validating and verifying digital forensic tools in terms of the data recovery function, the consideration of physical damage recovery techniques is outside the scope of this paper and is considered to be complementary to logical damage recovery techniques. Consequently, in the rest of this paper, data recovery refers to logical damage recovery unless otherwise stated.

Data recovery in the context of digital forensics has its peculiarities and differs from traditional data recovery in the computer science discipline. First, data recovery in the digital forensic context is a process by which digital evidence is recovered for use in court. Therefore, it should be conducted by certified investigators, conform to standard operating procedures, utilize tools that are validated and verified by the appropriate authorities, and be supervised and documented. Traditional data recovery does not have these requirements because its goal is to recover as much data as possible without concern for its forensic soundness. Second, the techniques used in traditional data recovery and the digital forensic context differ because of the forensic soundness issue. For example, in traditional data recovery, a corrupted main boot record may be repaired by laying a FAT2 over a FAT1 if the FAT2 is intact. However, this is not an appropriate forensic data recovery technique because the original evidence (FAT1) is modified. Instead, it would be necessary to repair the corrupted main boot record in duplicate (i.e., image). Finally, forensic data recovery embraces a broader view of recovering data than traditional data recovery and,

[101] Y Guo, J Slay and J. Beckett, Validation and verification of computer forensic software tools – Searching function, Digital Investigation, vol 6(S1), pp S12–S22, 2009

consequently, must consider issues (e.g., hidden data and trace data) that are beyond the purview of traditional data recovery.

The data recovery function is mapped by detailing its components, processes and relevant factors. Since the goal of data recovery is to retrieve data due to storage media abnormalities and/or intentional human manipulation, the function mapping is performed from three angles: (i) storage media; (ii) recovery object; and (iii) recovery reason.

1.5 REASONS FOR DATA RECOVERY

A data recovery method is used when data is unavailable. In the context of digital forensics, data is unavailable and must be salvaged for various reasons, including damage, corruption or hiding. From thepoint of view of the user (e.g., investigator), we assume that the data is unavailable because it is inaccessible or hidden. By inaccessible data, we mean that the user is aware of the existence of the data, but is unable to access it in a normal manner. On the other hand, hidden data is invisible to the user, and the user does not know of its existence.[102]

- ***Inaccessible data***

"Orphaned" files are inaccessible to users under normal operations. An orphaned file is one that no longer has a parent (the parent is the folder in which it was originally located). The term orphaned is a broad concept that includes deleted files. In most cases, orphaned files are deleted files, but a file can be orphaned when the association with its parent is lost through other means (e.g., byremoving a symbolic link in a Unix environment).

- ***Hidden Data***

In the digital forensic context, it may be necessary to recover data that has intentionally been hidden. Data hiding methods may be categorized as hardware-based or software-based, Hardware-based methods hide data in specific areas of storage media. For example, data on a hard disk may be stored in the HPA (host protected area), DCO (device configuration overlay), UPA (unused partition area) and inter-partition space.

[102] National Institute of Standards and Technology, Computer Forensics Tool Testing Program, Gaithersburg, Maryland <www.cftt.nist .gov>

Software-based methods hide data using the file system and/or operating system utilities . For example, modern hard disk controllers handle bad sectors without the involvement of the operating system by slipping (modifying the LBN (logical block number) to physical mapping to skip the defective sector) or remapping (reallocating the LBN from a defective area to a spare sector). For older hard disks that do not have this capability, the operating system and file system have to retain the ability to detect and mark defective sectors and clusters as damaged. This feature can be used to exclude undamaged clusters from normal file system activities and use them to hide data.

Software-based data hiding methods may also use ambient space. Slack space, which includes file slack space, volume slack space and partition slack space, are areas on the disk that cannot be used by the file system because of the discrete nature of space allocation. Data can be hidden in any of these locations.

1.6 REQUIREMENT SPECIFICATION

Requirements specification is the second step of the validation and verification framework. The data recovery function requirements are specified in the same way as the search function requirements in. The method of specifying requirements is highly abstract and generalized. We use italicized "variables" to reflect these variations.[103] Thus, when a requirement has to be changed, it is only necessary to adjust (add, delete or modify) the variables. Moreover, the requirements can be unwrapped when it is necessary to develop a specific test scenario in a reference set. For example, the requirement: "The tool shall be able to accurately recover inaccessible recovery objects" may be unwrapped and instantiated as "The tool shall be able to accurately recover deleted JPG files" or "The tool shall be able to accurately recover hidden data in file slack."

A digital forensic tool has the following eight requirements with respect to the data recovery function:

- The tool shall operate in at least one operational environment.

[103] RMcKemmish, What is forensic computing? Trends and Issues in Crime and Criminal Justice, no 118 <www.aic.gov.au/publications /tandi/ti118.pdf>

- The tool shall operate under at least one operating system.
- The tool shall operate on at least one type of storage media.
- The tool shall be able to accurately render system data.
- The tool shall be able to accurately recover inaccessible (recovery)objects.
- The tool shall be able to accurately recover hidden (recovery) objects.
- If there are unresolved errors when reconstructing data, then thetool shall report the error types and error locations.
- The tool shall report the attributes of the recovered data.

1.7 RECOVERED OBJECTS

File system data to be recovered belongs to one of four categories: system data, user data, metadata and trace data.[104]

- ***System data***

System data includes general hardware and software information. Data recovery techniques include hardware rendering and software (operating system and file system) rendering. Hardware rendering refers to the ability to accurately identify particular types of devices and media. This is accomplished through physical interaction with the device or media or by using metadata located on the device or media.

The goal of the operating system orfil e system rendering is to reveal the underlying structure. Operating systems andfile systems have a general structure, but each instance is unique. In addition, many of these systems are proprietary in nature and, as a result, are poorly documented (e.g., the detailed structure of NTFS has not been publicly released). Operating system andfile system rendering may specify where certain structures are found and the data unit size that enables file folders, data and metadata to be accurately retrieved. For example, thevolume label and the associated data are indicators of the method usedto create the allocated components of a device. Different file systemsrecord this information differently, so a digital forensic tool must be able to render the volume label(s) from a device or partition.

[104]Guo, Yinghua& Slay, Jill (2010) Data Recovery Function Testing for Digital Forensic Tools. IFIP Advances in Information and Communication Technology.

- ***User Data***

User data is the principal object of data recovery. User data are categorized as document, graphic, sound or Internet files. This classification is by no means exhaustive and will have to be updated constantly to accommodate new applications and file formats. Note that user data files may be in special forms (e.g., compressed and encrypted), which should be taken into account by forensic examiners.

- ***Meta Data***

Metadata is data that describes data or files. It includes data about where the file content is stored, file size, dates and times of the last read and write, and access control information. Metadata must be analyzed to determine details about a specific file or to search for a file that meets certain requirements.

- ***Trace Data***

Data recovery in the digital forensic context is a much broader concept than traditional data recovery. Trace data is the data that remains on the storage media after operations such as hard drive partitioning, formatting and file deletion . Trace data may not be substantial but may constitute important digital evidence. For example, file operations (e.g., creation, modification and deletion) leave traces in the form of temporary files. Most temporary files are deleted by the operating system after the file operations are completed. However, if a temporary file is deleted, its contents can be recovered if the clusters allocated to the file are not reallocated. Also, even if the allocated clusters are reallocated, file metadata (e.g., name and timestamp) may exist and may prove to be useful in a digital forensic investigation.

1.8 REFERENCE SET DEVELOPMENT AND TESTING

A reference set consists of test scenarios (cases) against which a digital forensic tool or its individual function is validated. The development of test scenarios is based on the specification of function requirements. Using the requirements specification, it is possible to establish a reference set for testing the data recovery function of various digital forensic tools. Since the functional requirements are specified in an extensible manner, the corresponding reference set is also extensible. This would enable practitioners, tool developers and researchers to identify

critical needsand to target deterministic reference sets.We have identfied eight requirements for the data recovery function. Since each requirement has several variables, multiple test scenarios have to be designed for each requirement. Each scenario represents a single instantiation of each variable. The following are some pilot samples of the reference set for the data recovery function:

- A deleted JPG file in a FAT32 file system on an IDE hard disk.
- A deleted JPG file in an NTFS file system on a SCSI hard disk.
- A deleted WAV file in a UDF file system on a CD.
- A deleted Microsoft Word file in an FFS file system on flash memory.
- A deleted compressed HTML file in an NTFS file system on anIDE hard disk.
- An encrypted MP3 file in a FAT32 file system on an ATA harddisk.

1.9 CONCLUSION

Mapping the fundamental functions of the digital forensic discipline is a powerful approach for creating a function-oriented validation and verification paradigm for digital forensic tools. The utility of the approach is demonstrated in the context of the data recovery function via the specification of data recovery requirements and a reference set for testing tools that implement the data recovery function. Validating a digital forensic tool is reduced to testing the tool against the reference set. Compared with traditional testing methods, this testing paradigm is extensible and neutral and transparent to specific tools and tool versions.

1.10 LET'S SUM UP

More work remains to be done to complete the validation paradigm. Although the methodology holds promise, it needs to be tested extensively to evaluate its utility and identify potential weaknesses and shortcomings. Tests would have to be implemented against popular tools such as EnCase and FTK. A quantitative model is also required to evaluate the results of validation and verification. Metrics are needed to measure the accuracy and precision of testing results, and it is necessary to specify rules for judging the validity of digital forensic tools. Is a tool validated only

when it passes all the test cases? Or is a tool validated when it passes the test cases for certain scenarios?

It is important to recognize that numerous variables are involved in function requirements specification and that the corresponding reference set can be very large. Indeed, the number of possible combinations for validating a single function in a digital forensic tool may well be in the thousands (even discounting the different versions of the tool). Interestingly, this problem is also faced by the Computer Forensics Tool Testing (CFTT) Program created by the National Institute of Standards and Technology (NIST) to validate and verify digital forensic tools.

1.11 FURTHER READING

- E. Huebner, D. Bem and C. Wee, Data hiding in the NTFS file system, Digital Investigation, vol. 3(4), pp. 211–226, 2006.
- Y. Guo, J. Slay and J. Beckett, Validation and verification of computer forensic software tools – Searching function, Digital Investigation, vol. 6(S1), pp. S12–S22, 2009.
- R. McKemmish, What is forensic computing? Trends and Issues inCrime and Criminal Justice, no. 118 (www.aic.gov.au/publications/tandi/ti118.pdf), 2002.
- G. Mohay, A. Anderson, B. Collie, O. de Vel and R. McKemmish,Computer and Intrusion Forensics, Artech House, Norwood, Massachusetts, 2003.
- A. Pal and N. Memon, The evolution offile carving, IEEE SignalProcessing, vol. 26(2), pp. 59–71, 2009.

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is data recovery?

Data recovery is generally regarded as the process of salvaging data partially or completely from damaged, failed, corrupted or inaccessible storage media.

2) How is the function mapping being performed?

The function mapping is performed from three angles: (i) storage media; (ii) recovery object; and (iii) recovery reason.

3) What are the requirements of digital forensic tool for data recovery function?

A digital forensic tool has the following eight requirements with respect to the data recovery function:

- The tool shall operate in at least one operational environment.
- The tool shall operate under at least one operating system.
- The tool shall operate on at least one type of storage media.
- The tool shall be able to accurately render system data.
- The tool shall be able to accurately recover inaccessible (recovery)objects.
- The tool shall be able to accurately recover hidden (recovery) objects.
- If there are unresolved errors when reconstructing data, then thetool shall report the error types and error locations.
- The tool shall report the attributes of the recovered data.

4) What is a reference set?

A reference set consists of test scenarios (cases) against which a digital forensic tool or its function is validated.

1.13 ACTIVITY

Explain briefly the process involved in data recovery and the tools required for digital forensic with respect to recovered objects and testing? (800-1000 words)

Unit 4: Avenues for Prosecution and Government Efforts

4

SUBJECT CODE: PGDCL 104

DIGITAL RECORDS AND CYBER FORENSICS

BLOCK 3 – ROLE AND ANALYSIS OF CYBER FORENSICS

UNIT 4 – AVENUES FOR PROSECUTION AND GOVERNMENT EFFORTS

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 The evolution of computer-specific statutes

1.4 Computer Fraud and Abuse Act, 1986

1.5 National Information Infrastructure Protection Act, 1996

1.6 Evolving Child Pornography Statutes

1.7 Identity Theft and Assumption Deterrence Act, 1998

1.8 Identity Theft Enforcement and Restitution Act, 2008

1.9 Automated Targeting System (ATS)

1.10 Terrorist Surveillance Program

1.11 Virtual Global Taskforce

1.12 Let's sum up

1.13 Further reading

1.14 Check your progress: Possible answers

1.15 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The evolution of computer-specific statutes
- Terrorist surveillance program
- Virtual Global Taskforce

1.2 INTRODUCTION

The advent of computer crime has resulted in a myriad of problems for law enforcement administrators. The lack of resources available to small agencies, the traditional apathy toward nonviolent crime, and the reluctance of legislative action have enabled many computer criminals to act with virtual impunity. While it is anticipated that an increase in technology-specific legislation and the modification of extant statutes are forthcoming, lawmakers should evaluate existing federal and state law for prosecutorial avenues currently available. This would empower local agencies and reduce demands on federal agencies.[105]

Traditionally, state and local officials have been forced to rely exclusively on the expertise of better-trained, better-funded federal agencies. Unfortunately, these agencies are incapable of addressing every call for assistance. In addition, they are often unwilling to expend resources on crimes which do not constitute threats to institutional security, the economic infrastructure, the exploitation of children, individual safety, or violation of federal law. (It is unlikely, for example, that a federal agency would assist law enforcement in cases constituting misdemeanour offenses or those offenses which appear to be minor—e.g., installation of Back Orifice on a personal computer, a currently contained virus which destroyed two computers.) Law enforcement administrators should carefully evaluate state statutes. When used creatively, many can be directly applied to criminal activity involving computers. Remember, the method of execution is not an essential element in criminal law. Intent, action, and illegality are inherent in every case of larceny, for example. The method is irrelevant. Thus, an individual who utilizes a computer to steal money from a bank is just as culpable as the individual who resorts to physical theft. At the

[105] Adams, D (2003, December 16) Police prove a match for electronic foe. The Sydney Morning Herald. Retrieved on 28th January 2015 from <http://www.smh.com.au/articles/2003/12/15/1071336882279.html?from=storyrhs>

same time, criminal mischief or vandalism statutes may be utilized to prosecute an individual who remotely alters data. Investigators and administrators must be encouraged to look for the obvious! While there are a variety of statutes which have been enacted to specifically address technological crime, traditional statutes should be utilized where the former is lacking.

1.3 THE EVOLUTION OF COMPUTER-SPECIFIC STATUTES

While many state legislatures have been slow to enact computer-specific statutes, U.S. Congress has reacted more quickly. Thus, measures enabling the prosecution of electronic fraud, hacking, and the theft of intellectual property may be found at thefederal level. Unfortunately, this legislation has been buffeted by a variety of legal challenges, the language characterized by jurists as vague and ambiguous.[106] Such efforts can be traced back to 1977 when Senator Abraham Ribicoff (Connecticut) introduced the Federal Computer Systems Protection Act (FSCPA). Although the bill died in committee, it was responsible for initiating dialogue and communication about the threat and potentiality of computer crime.

1.4 COMPUTER FRAUD AND ABUSE ACT, 1986

Originally known as the Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA), Section 1030 of Title 18 of the U.S. Code quickly became the federal government's main weapon in fighting computer crime. Known as the hacking statute, the act in its original form was very narrow in scope, making it a felony to knowingly

> [a]ccess a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation. Second, the 1984 Act made it a misdemeanor knowingly to access a computer without authorization, in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency. Third, the 1984 Act made it a misdemeanour knowingly

[106]Nicholson, Laura J; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey" American Criminal Law Review, 37(2): 207–210

to access a computer without authorization, or in excess of authorization, in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer. The 1984 Act also made it a crime to attempt or to conspire to commit any of the three acts described above.

This legislation proved to be largely ineffective due to the ambiguity of the statutory language and an overemphasis on financial information. (Only one person was successfully prosecuted under the original provisions.)Finally, the 1986 revisions specifically targeted hackers by criminalizing password trafficking.[107]

The act was also used to prosecute early hackers, Herbert Zinn (aka Shadowhawk) and Kevin Mitnick. Shadowhawk was an 18-year-old high school dropout and hacker extraordinaire. Herbert Zinn considered a juvenile at the time of his arrest, was sentenced to nine months and fined $10,000 for breaking into computers of various organizations ranging from NATO to the U.S. Air Force. In addition, Zinn stole 52 AT&T programs valued at over $1 million. Provisions under the act could have resulted in a prison term of 20 years for an adult charged with the same range of offenses. Unlike Zinn, Kevin Mitnick, one of the most infamous hackers in history, had a criminal history the length of which rivals that of many organized crime figures. His successful conviction under this act was a result of his theft of programs valued at more than $1 million from Digital Equipment Corporation and the illegal manipulation of MCI service codes. Since its inception, the act has been modified several times, primarily to clarify terms.

1.5 NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT, 1996

While the CFAA was successfully used to prosecute hackers and individuals who exceeded their authorized use, it contained significant limitations in that it only involved those cases in which computer data was a target. It neither included other offenses committed via or in conjunction with computer technology nor included noninterest computers. To remedy this, Congress passed the National Information Infrastructure Protection Act (NIIPA).[108] Originally conceived in 1996,

[107]Pastrikos, Catherine (2004). "Identity Theft Statutes: Which Will Protect Americans the Most?" Albany Law Review, 67(4): 1137–1157

[108] 18 U S C § 1030

NIIPA amended the CFAA to provide for any computer attached to the Internet even if the said computer was not one defined as a federal interest computer or if multiple computers were located in one state. In addition, NIIPA identified broad areas of computer-related crime which involve either accessing computer systems without/or in excess ofauthorization or causing damage to computers.

These modifications served to close numerous loopholes in the original legislation. By extending protection to all computers connected to the Internet, NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers. In addition, by removing the trespass requirement and adding an intent or recklessness element, NIIPA provides for the prosecution of insiders who intentionally damage computers. The act further provides for the prosecution of individuals trafficking in passwords or those who attempted to extort money or values from an individual or entity by threatening computer harm. Finally, and perhaps more importantly, NIIPA successfully eliminates several defenses predicated on intent, implied authorization, or value of access. More specifically, NIIPA requires only an intent to access not an intent to cause damage. Thus, individuals attempting to access a protected computer may be prosecuted even if their motivation was not fiduciary.

1.6 EVOLVING CHILD PORNOGRAPHY STATUTES

Although a variety of laws have been enacted to combat the increase in technological crime, none are more emotionally charged than those dealing with child pornography. Beginning in 1977, Congress has attempted to eliminate child pornography. Originally criminalized at the federal level with the Protection of Children against SexualExploitation Act of 1977 (PCSE), Congress has periodically revised the legislation to protect children from sexual exploitation in keeping with emerging legal doctrine. However, lower courts have remained divided on new legislation, and the Supreme Court has denied cert on the majority of cases. Traditionally, evaluations of child pornography statutes relied primarily on two Supreme Court decisions, whose interpretation of and application to emerging laws have been diverse.[109]

[109] Stevens, Gina and Doyle, Charles (2003) Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: 98-326. Retrieved from <www.epic.org>on March 23, 2012.

In 1982, the Supreme Court evaluated free-speech challenges to child pornography and found them wanting ***(New York v. Ferber).***[110] Uncharacteristically emphatic,the Court ruled that child pornography was outside the scope of the First Amendment, and allowed states to enact blanket prohibitions against visualizations of children engaged in sexual situations. The Child protection act of 1984 (CPA) incorporated this decision. Although the CPA lacked technological specificity, it was widely used against online offenders until the emergence of the Child Protection and Obscenity act of 1988. While both of these acts were designed to protect children from exposure to and inclusion in material deemed to be obscene, these and future acts are continuously challenged by freespeech advocates. At the same time, the Supreme Court has remained resolutely silent.

The Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act. Although it sought to reinstate the original provisions housed within the CPPA, it also included a variety of other measures designed to protect children both online and offline. The most important of these included the following:

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.7 IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT, 1998

In October 1998, the Identity Theft and Assumption Deterrence Act (ITADA) waspassed by Congress. It was the first act to make the possession of another's personal identifying

[110]*New York v Ferber*458 U S 747

information a crime, punishable by up to 20 years in prison. More specifically, the act stated that it is unlawful if an individual,[111]

> [k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

In addition, the law expanded the traditional definition of "means of identification" to include:

- name, social security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer-identification number;
- unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- unique electronic identification number, address, or routing code; or
- telecommunication identifying information or access device.

1.8 IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT, 2008

In 2008, Congress formally recognized the financial impact of identity theft by passingthe identity theft enforcement and restitution act. Among other provisions, the act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization including lost wages and credit rehabilitation.[112]

1.9 AUTOMATED TARGETING SYSTEM (ATS)

[111] Seifert (2007) Data Mining and Homeland Security

[112]Broadhurst, Roderic (2006) "Developments in the Global Law Enforcement of Cyber-Crime" Policing: An International Journal of Police Strategies and Management, 29(3): 408–433

The Automated Targeting System (ATS) was developed by the Department of Homeland Security within the Treasury Enforcement Communications System. It was designed to screen travellers entering the United States by automobile, aeroplane, or rail. Housed within the Bureau of Customs and Border Protection (CBP), ATS assesses risks for cargo, conveyances, and travellers. There are six categories, or modules, of activity:

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

Like other data-mining practices by law enforcement, ATS has been harshly criticized by privacy advocates. In 2006, a suit was filed to suspend the systems as it applied to individuals, or, in the alternative, fully apply all Privacy Act safeguards to any person subjected to the system.Although it was originally designed to enhance customer service in the private sector through customizing profiles of individual shoppers, it has increasingly been employed by criminals and law enforcement alike.[113]

1.10 TERRORIST SURVEILLANCE PROGRAM

First disclosed to the public in December 2005 via a news report, the Terrorist Surveillance Program has been employed by the National Security Agency (NSA) since 2002. Among other things, the program includes the domestic collection, analysis, and sharing of telephone call information. According to statements issued by the president and the Department of Justice, the program is reserved for international calls with links to al Qaeda or related terrorist groups and requires review and reauthorization every 45 days. Privacy advocates have repeatedly expressed concerns over the potential for abuses. Recently, such concerns were validated when it was

[113] Frost and Sullivan (2003) "U S CALEA Market Insight: 6841–63" Retrieved from <http://www.corp.att.com/stateandlocal/docs/US_ CALEA_Market_Insight.pdf on February 12, 2013>

revealed that the NSA had contracted with AT&T, Verizon, and BellSouth to collect information about domestic telephone calls. Although the content of such disclosures is not entirely clear, the compromise of privacy expectations and subsequent erosion of public trust occurred.

CASE STUDY – PRIVACY IN IRAN

In 2010, Nokia Siemens Network was sued by Iranian dissidents who alleged that Nokia had provided the Iranian regime with devices which monitored, eaves-dropped, filtered, and tracked mobile phones.[114] The suit was filed after Isa Sakarkhiz, a prominent Iranian journalist who was instrumental in illuminating Iran's oppression of the press was arrested by government agents who had tracked his mobile phone using Nokia's Intelligence Solutions tool which had been sold to the state-owned telecommunicationsprovider. This Nokia system, which was sold and specifically modified to the government's needs, was composed of (1) a monitoring area which provided for the centralized deep packet inspection of both voice and data communications, and (2) an intelligence area which provided for real-time data mining. Although Nokia claims to have abandoned the software which provides for monitoring of communications, they have declared themselves immune from responsibility as they are a corporation.[115]

1.11 VIRTUAL GLOBAL TASKFORCE (VGT)

In 2003, the Virtual Global Taskforce was created as a collaborative effort between the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre (UK), the Royal Canadian Mounted Police, the U.S. Department of Homeland Security, and Interpol.[116] It is designed to deliver low-cost, high-impact initiatives that deter pedophiles and prevent the online exploitation of children. By reducing the confidence of potential perpetrators through the removal of perceptions of anonymity, the group aims to deter online misconduct. Their most notable initiative is to know as Operation Pin. This program involves a Web site which claims to contain images of child exploitation and pornography. Visitors to the site who attempt to

[114] United Nations (2000) "United Nations Manual on the Prevention and Control of Computer-related Criteria"
[115] Department of Defense (May 20, 2003) Report to Congress Regarding the Terrorism Informational Awareness Program, Detailed Information. Retrieved from<www.epic.org on March 23, 2012>
[116]<http://www.virtualglobaltaskforce.com>the homepage of the Virtual Global Taskforce. The group, dedicated to the prevention and prosecution of online child abuse, provides access to the latest news regarding online predators and law enforcement successes

download images are confronted by an online law enforcement presence and informed that they have committed a criminal offense and that information about them has been forwarded to appropriate authorities.

1.12 LET'S SUM UP

Although recognition of the insidious nature of computer crime is increasing, much work remains to be completed on all levels of government. Legislation and the codification of computer criminality must keep abreast of emerging technology. Until such a time, investigators should look to traditional statutes to prosecute individuals committing traditional crimes via electronic means.

Even in areas where state, local, and federal government agencies have enacted regulations to specifically address online criminal behavior, some activity is sure to be over-looked. Thus, law enforcement officials must continue to evaluate the applicability of traditional legislation. The Federal Wire Fraud Act, for example, enables prosecutors to pursue individuals illegally transferring funds, accessing bank computers, and the like. While most computer-specific legislation has tended to be enacted on the federal level,state and local agencies may be able to implement generic statutes of enforcement. For example, although many states have not formally encoded electronic vandalism statutes, innovative departments may still pursue individuals responsible for computer worms or viruses through criminal mischief and destruction of property codes. Local and state law enforcement officials should carefully evaluate local regulations and identify applicable statutes.

1.13 FURTHER READING

- Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798. January 18, 2007.
- International Review of Criminal Policy—United Nations Manual on the Prevention and Control of Computer-Related Crime. Retrieved from http://www.uncjin.org/Documents/EighthCongress.html on February 12, 2013.

- Nicholson, Laura J.; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey." American Criminal Law Review, 37(2): 207–210.
- Stevens, Gina and Doyle, Charles (2003). Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: #98-326. Retrieved from www.epic.org on March 23, 2012.
- Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798.
- Poulsen, Kevn (2005). "FBI Retires Its Carnivore." Security Focus. Retrieved from www.securityfocus.com on March 23, 2012.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the main aim/objective of the National Information Infrastructure Protection Act, 1996?

NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers.

2) What are the six categories of Automated Targeting System?

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

3) What was the reason behind the enactment of Identity Theft Enforcement and Restitution Act, 2008?

The act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization, including lost wages and credit rehabilitation.

4) **Short notes on the evolution of child pornography?**

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.15 ACTIVITY

Explain briefly the evolution of different statutes that was brought to light with respect to computer-based crimes and the after-effects with respect it? Also, How may traditional statutes be applied to the contemporary phenomenon of computer crime? (1000 words)

Block 4

Cyber Forensics from Law Enforcement Perspective

Unit 1: Computer Forensics and the Process of Confiscation

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Concept of Computer Forensic

1.4 Collecting Evidence at Individual's Level

1.5 Collecting Evidence at ISP Level

1.6 Process of Cyber Forensic

1.7 Problems with Preserving Computer Evidence

1.8 Various branches of Digital Forensics

1.9 Process of Confiscation

1.10 Admissibility of Digital Evidence

1.11 Conclusion

1.12 Let's sum up

1.13 Further reading

1.14 Check your progress: Possible answers

1.15 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Concept of computer forensics
- Techniques in computer forensic
- Preserving Computer Evidence

1.2 INTRODUCTION

The term ***'computer forensic'*** was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a branch of forensic science which is devised to identify local preserve of extract digital information from the computer system to produce and store evidence of the cybercrime beforethe law court.[117]Dr Clifford Stall, an astronomer and professor in theUniversity of Berkeley has defined - computer forensic, as that branch offorensic science wherein cybercrime investigation and analysistechniques are applied to determine potential legal evidence in acomputer environment. Internet-related forensics broadly cover threeareas, namely (i) computer forensics, (ii) cyber forensics, and (iii)software forensics.

Cyber forensics plays a crucial role in solving crimes. The collection of forensic evidence serves an important key role that sometimes it is the only way to establish or exclude any case between suspect and victim or crime scene, eventually to establish a final verdict. As Internet technologies associate with us into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted which helps in the investigation process.

1.3 CONCEPT OF COMPUTER FORENSIC

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)***by using either a dial-up connection or a leased line/broadband/ mobile network facility.[118]

There are two levels at which evidence of Internet usage exists:

a) Individual Level
   - On an individual's own computer, computer system or computer network.
   - On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

[117]Rohas N, "Understanding Computer Forensics", Asian school of cyber law, 2009
[118] Cyber Forensics and Indian Approach
<http://ptlb.in/cfrci/?p=15>

- On the service of an individual's ISP.

1.4 COLLECTING EVIDENCE AT INDIVIDUAL'S LEVEL

Computers usually store text, graphic, image files, e-mails messages etc. in the hard disk during its routine use. User may keep on deleting the unwanted material regularly to free up disk space. Similarly, Chat rooms, Internet Relay Chat (IRC), Internet telephony sessions are real-time discussions happening on the Internet; it is optional for the user to maintain logging files of these sessions.[119]

Caching means copying of a web page/site and storing that copy for the purpose of speeding up subsequent access. It ensures that the load on the servers of origin will be reduced as they can be accessed from the cached servers. With the help of browser software, a user can retrieve any web page from the computer's cache memory rather than going back to the original source site. From the legal standpoint, the information saved in a web-browser cache whether or not intentionally retained constitutes ***'possession'.***

1.5 COLLECTING EVIDENCE AT ISP LEVEL

Logs maintained by the ISPs of the users using dial-up/leased line/ broadband/mobile-Internet connections to connect to ISP indicate the time and duration of Internet usage/connectivity along with the IP address. It will corroborate other types of evidence that has already been gathered during the investigation. Admissibility of such evidence cannot be questioned as it clearly highlights not only the time and duration of computer's Internet usage/connectivity but also the fact that during a specific time period, the user's computer had been working as a sort of *'computer network'*. It is important to note that ISPs under the licensing conditions are collecting traffic data in the form of IP addresses, machine IDs (Mac ids), date and time (of communication), size of data (received/sent) and other related information.

[119] Cyber Forensic Investigation Solutions in India Are Needed <http://ptlb.in/cfrci/?p=9>

1.6 PROCESS OF CYBER FORENSIC

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.[120]
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.
- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.
- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

1.7 PROBLEMS WITH PRESERVING COMPUTER EVIDENCE

Preserving evidence is not an easy task.[121] There exist both human and technical barriers to the evidence gathering mechanism. One must be aware of such limitations:

- Some of the facilities within the browsers to save WWW pages to the hard disk are imperfect- as it may save the text but not the associated images.

[120] Cyber Forensics
<http://www.cyberlawsindia.net/computerforensics1.html>
[121] Sadiku, Matthew &Tembely, Mahamadou& Musa, Sarhan.(2017) Digital Forensics. International Journal of Advanced Research in Computer Science and Software Engineering

- In case of some very complex pages, involving *'frames'* and *'templates'*, there could be a perceptible difference in what is seen on screen and what is saved on the hard disk.
- The method used to save a file to the hard disk may not carry any individual labelling, which shows where and when it was obtained. The problem with such saved files is that they could be easily modified or forged.
- It is difficult to tell when a specific page was last acquired due to the browser cache facility. Thus if one examines a whole series of cached pages, it is not easy to pinpoint which page came first and which later.
- It should not be forgotten that many ISPs use proxy servers to speed up the delivery of popular pages. Thus a user of such an ISP may not be sure that what he has received on his computer is the latest version from the source computer (website) as opposed to an earlier cached version held by his ISP.

1.8 VARIOUS BRANCHES OF DIGITAL FORENSICS

Digital Forensics has a very wide scope.[122] The branches of digital forensics are as follows:

a) Disk Forensics

Disk Forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, FireWire devices, CD, DVD, Flash drives, Floppy disks etc.

b) Printer Forensics

Printed material is a direct accessory to many criminals and terrorist acts. In addition, printedmaterial may be used in the course of conducting illicit or terrorist activities. In both cases,the ability to identify the device or type of device used to print the material in question wouldprovide a valuable aid for law enforcement and intelligence agencies.

c) Network Forensics

Network forensics is a branch of digital forensics that focuses on the monitoring and analysisof network traffic. Network forensics is the process of gathering and examining raw

[122] I. Resendez, P Martinez, and J Abraham, "An Introduction to Digital Forensics," June 2014, <https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics>

dataof network and systematically tracking and monitoring the traffic of the network to make sure ofhow an attack took place.

Traffic is usually intercepted at the packet level, and either stored for later analysis or filteredin real-time. Unlike other areas of digital forensics network data is often volatile and rarelylogged, making the discipline often reactionary. Security professionals routinely use suchtools to analyze network intrusions not to convict the attacker but to understand how theperpetrator gained access and to plug the hole.

It also helps to investigate offences after the event, determine how they occurred and identify the party or parties responsible. A digital forensic investigator will gather network based evidence from a particular computing device in the network so that it can be presentedin court, conducting a thorough digital investigation and building a documented chain ofevidence.

d) Mobile Device Forensics

Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially thosewith advanced capabilities, are a relatively recent phenomenon, not usually covered inclassical computer forensics. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. Developing anunderstanding of the components and organization of cell phones is a prerequisite to understanding the criticalities involved when dealing with them forensically. Similarly, features of cellular networks are an important aspect of cell phone forensics, since logs of usage and other data are maintained therein. Cell phone forensics includes the analysis of both SIM and phone memory, each requires a separate procedure to deal with.

It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.

e) Database Forensics

Database forensics is a branch of digital forensics relating to the forensic study following the normal forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in a servers RAM requiring live analysis techniques.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify theactions of a database user. Alternatively, a forensic examination may focus on identifyingtransactions within a database system or application that indicate evidence of wrongdoing,such as fraud.

Third-party software tools which provide a read-only environment can be used to manipulateand analyze data. These tools also provide audit logging capabilities which providedocumented proof of what tasks or analysis a forensic examiner performed on the database.

f) Digital Music Device Forensics

Large storage capacities and personal digital assistant (PDA) functionalities have made the digital music device a technology that should be of interest to the cyber forensic community.The digital music revolution has also seen the digital music device become a commonhousehold item. It is only a short time until they too make a natural progression into thecriminal world. This progression has already begun. Some of the hard-drive-based deviceshave capacities upwards of 60GB. With this much storage space for music, developers havebranched out and included features like a calendar and contact book (Apple iPod-Musicand more). These devices are simply a portable hard drive and have the ability to store othertypes of files besides music; such as documents or pictures.

An employee could take sensitive information by using the capabilities of a digital music device. Suspects could potentially store critical evidence on these types of devices. It must bedetermined if current frameworks of cyber forensic science are applicable and to what extentcurrent guidelines can be applied to digital music device forensics.

g) Scanner Forensics

A large portion of digital image data available today is created using acquisition devices suchas digital cameras and scanners. While cameras allow digital reproduction of natural scenes,scanners are used to capture hardcopy art in more controlled scenarios. For a forensic approach, a non-intrusive scanner model identification, which can be further extended to authenticatescanned images is a necessity.

Using only scanned image samples; a robust scanner identifier should determine the brand/model of the scanner used to capture individual scanned images. A proposal for such ascanner identifier is based on statistical features of scanning noise. Scanning noise of the images can be done from multiple perspectives, including image denoising, wavelet analysis,and neighbourhood prediction, and obtain statistical features from each characterization. Thesame approach can be extended to digital cameras and other imaging devices. The mostsignificant challenge is that ***"analytical procedures and protocols"*** are not standardized nor dopractitioners and researchers use the standard terminology.

The technology change will result in new devices emerging in the digital world. Whenever anew digital device enters the market a forensic methodology has to evolve to deal with it. This phenomenon will expand the field of device forensics.

h) PDA Forensics

In the modern era, Personal Digital Assistants (PDAs) are getting immensely popular. They are no longer meagre electronic devices holding personal information, appointments and address book. Modern PDAs are hybrid devices integrating wireless, Bluetooth, infrared, WiFi, mobile phone, camera, global positioning system, basic computing capabilities, Internet etc., in addition to the standard personal information management features.

Investigating crimes involving PDAs are more challenging than those involving normal computers. This is mainly because these devices are more compact, battery-operated and store data in volatile memory. A PDA is never really turned off as long as it has sufficient battery power. Evidence residing in PDA is of highly volatile in nature. It can be easily altered or damaged without getting noticed. In order to collect such evidence and ensure its admissibility in a court of law, sound forensic techniques and a systematic approach are needed. A standard forensic model for PDAs, which provides an abstract reference

framework is particularly important in digital crime investigations. In addition to law enforcement officials, such a model can also benefit IT auditors, information security experts,IT managers and system administrators, as often they are the first responders related to anysort of computer crime in an organization.

1.9 PROCESS OF CONFISCATION

Section 76 of the Information Technology Act, 2000 highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders or regulations made thereunder are liable to be confiscated.[123]

The proviso to the section further highlights that in case if the person concerned in whose possession, power or control computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device is found, establishes to the satisfaction of the court that he was in no way responsible for any of the contraventions, the adjudicating court not to confiscate such devices, under such circumstances. In such a case, the court may make such other order authorized by this Act, against the person contravening provisions of this Act, rules, orders or regulations made thereunder.

1.10 ADMISSIBILITY OF DIGITAL EVIDENCE

Digital evidence usually takes the form of writing or at least a form which can be analogized to writing, it must be authenticated and satisfy the requirements of the Best Evidence Rule.

The proponent of the evidence need not present testimony by a programmer, but should present some witnesses who can describe how information is processed through the computer and used by the organization.

[123] N Kumari and A KMohapatra, "An insight into digital forensics branches and tools," Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016

With regard to hearsay, most courts have dealt with the objection to the introduction of computer records by relying on the business record exception. Such an approach may work for audit logs, provided they satisfy the rule, which might not be the case for computer records collected as part of an investigation rather than as the result of a routine, periodic process. The following are some guidelines to preserve admissibility of digital evidence:

- Upon seizing digital evidence, action should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person must be forensically competent.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

In the case of ***P.V. Anwar v P.K.Basheer,***[124]the Court in ***PARAGRAPH 24 OF ITS JUDGMENT***held that the electronic evidencewhich is a primary document can be admitted without producing certificate and thereis no obligation to satisfy the condition laid down in Section 65B of the Evidence Act, 1872. If that electronicrecord satisfies the condition under Section 62 then it can be unequivocally admitted as evidence.The same will not be covered either under Section 65A or 65B of the Evidence Act, 1872.Primary evidence is a ***'document'***which is defined under Section 3 of Evidence Act, 1872.[125]

1.11 CONCLUSION

Cyber forensics plays a significant role in the criminal justice systemas we continue to incorporate a range of technologies into our everyday lives. Evidence of allmost the types of crime is increasingly found in digital devices that either the perpetrator orthe victim used. As a

[124]*P V Anwar v P K Basheer* [2014] 10 SCC 473

[125] M Reith, C Carr, and GGunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol 1, no 3, Fall 2002

result of this potential evidence which did not exist in the past,investigators of conventional crimes increasingly need to consider any digital evidence thatmay be available.

In addition, Security professionals routinely use such tools to analyze network intrusions notto convict the attacker but to understand how the perpetrator gained access and to plug the hole. Data recovery firms rely on similar tools to resurrect files from drives that have been inadvertently reformatted or damaged.

1.12 LET'S SUM UP

In this chapter, we have studied the concept of computer forensic along with how the evidence is collected at each level. We also studied the process of cyber forensic and the problems faced in preserving the evidence. Finally, we ended the discussion with the process of confiscation and admissibility of digital evidence.

1.13 FURTHER READING

- The Role and Impact of Forensic Evidence in the Criminal Justice Process by JosephPeterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010
- Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies byTeri A. Cummins Flory (Purdue University),2016
- STANDARD OPERATING PROCEDURE OF DIGITAL EVIDENCECOLLECTION (Digital Forensics Department, CyberSecurity Malaysia)

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber forensics?**

   The term '*computer forensic'* was coined for the first time by the International Association of Computer Specialists (IACS) in Oregon (USA) in the year 1191. It is a

branch of forensic science which is devised to identify local preserve of extract digital information from thecomputer system to produce and store evidence of the cybercrime before the law court.

2. Explain the concept of Computer Forensic?

An individual uses his computer to connect the internet via an ***Internet Service Provider (ISP)*** by using either a dial-up connection or a leased line/broadband/ mobile network facility.

There are two levels at which evidence of Internet usage exists:

a) Individual Level

- On an individual's own computer, computer system or computer network.
- On the websites assessed by the individual using his own computer, computer system or computer network and

b) ISP Level

- On the service of an individual's ISP.

3. Explain the process of cyber forensic?

The process of cyber forensic is as follows:

- As soon as the crime is reported and is registered with the police, the investigation starts and data is collected from the place of crime/computer system and is examined using forensic techniques.
- The computer system seized is examined thoroughly to find out the digital data which can act as evidence.
- Important data which can help as a clue or evidence can remain hidden in different file formats like deleted files, hidden files, password-protected files, log files, system files etc.
- After all the information is gathered from the computer system the original form of evidence is recovered. It must very importantly be kept in mind that never to harm the originally recovered data while applying forensics.

- Create a mirror image of the original evidence using a different mechanism like bitstream etc. and use this mirror image of the original evidence. Never tamper the original copy of evidence for the investigation.
- Digital evidences are highly volatile and can be easily misinterpreted so care must be taken be.
- Enough supporting data/information must be gathered before presenting the digital evidence in front of the court of law.

4. What are the various branches of digital forensics?

- Disk Forensics
- Printer Forensics
- Network Forensics
- Mobile Device Forensics
- Database Forensics
- Digital Music Device Forensics
- Scanner Forensics
- PDA Forensics

1.15 ACTIVITY

Explain the different branches of digital forensics with illustrations along with the procedure for admissibility of electronic evidence and case laws with respect to it? (1500-2000 words)

Unit 2: Relevance of Indian Evidence Act to Cyber Forensics

2

SUBJECT CODE – PGDCL 104

DIGITAL RECORDS AND CYBER FORENSICS

BLOCK 4 – CYBER FORENSICS FROM LAW ENFORCEMENT PERSPECTIVE

UNIT 2 – RELEVANCE OF INDIAN EVIDENCE ACT TO CYBER FORENSICS

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Indian laws relevant to cyber forensics
1.3 Introduction to Indian Evidence Act
1.4 Amendments to Indian Evidence Act with respect to Electronic Evidence
1.5 Evidentiary value of electronic records
1.6 Let's sum up
1.7 Further reading
1.8 Check your progress: Possible answers
1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The different laws with respect to cyber forensics

- Relevance of Indian Evidence Act
- Amendments made in Indian Evidence Act for the recognition of digital evidence

1.2 INDIAN LAWS RELEVANT TO CYBER FORENSICS

Cyber forensics is becoming vast due to the use of technology in the commitment of a crime. Technological advancements have brought convenience in many daily activities. Now a day's human is living in two interrelated worlds namely Real World and Cyber World. Any act of a human is likely to create multiple traces in both worlds and that's why cyber forensics is not only related cybercrime but also very well utilised in traditional crime investigation. This resulted in the need of amendments in existing laws of the real world. IT Act 2000 is mainly enforced for legal recognition of electronic records in cyberspace.[126]

1.3 INTRODUCTION TO INDIAN EVIDENCE ACT

The Indian Evidence Act, 1872 resulted in changes in the definition of evidence because of the IT Act 2000. These two acts are directly related to cyber forensics in India. Cyber forensics and related investigation procedures have also led to some amendments in IPC and CRPC. In many circumstances, IT Act is having an overriding effect over IPC and CRPC.[127]

With the help of evidence, facts related to the incident are established at trial. Indian Evidence Act contains a set of rule and related issues governing the admissibility of evidence in the Indian Courts of Law. It has introduced a standard set of law applicable to all Indians. This act is divided into 3 parts and there are 11 chapters in total.

PART 1

Part 1 deals with relevancy of the facts. There are two chapters under this part: the first chapter is a preliminary chapter which introduces to the Evidence Act and the second chapter specifically deals with the relevancy of the facts.

PART 2

[126]Shrivastava, Gulshan& Sharma, Kavita&Khari, Manju&Zohora, Syeda. (2018) Role of Cyber Security and Cyber Forensics in India

[127] Ahmad, Farooq, Cyber Law in India (Law on Internet), Pioneer Books

Part 2 consists of chapters from 3 to 6. Chapter 3 deals with facts which need not be proved, chapter 4 deals with oral evidence, chapter 5 deals with documentary evidence and chapter 6 deals with circumstances when documentary evidence has been given preference over the oral evidence.

PART 3

The last part, that is part 3, consists of chapter 7 to chapter 11. Chapter 7 talks about the burden of proof. Chapter 8 talks about estoppels, chapter 9 talks about witnesses, chapter 10 talks about the examination of witnesses, and the last chapter which is chapter 11 talks about improper admission and rejection of evidence.

The Evidence Act provisions can be divided into 2 categories:

- Taking the evidence (By Port) - This means to take the evidence for the facts. The fact means the things which are said before the court in connection with the matter. These facts are given to the court either orally or documentary (also electronic documents).[128]
- Evaluation – In evaluation court check whether the facts produce are capable to prove the evidence. Forensics plays a vital role in the evaluation phase.

1.4 AMENDMENTS TO INDIAN EVIDENCE ACT WITH RESPECT TO ELECTRONIC EVIDENCE

Indian evidence Act is applicable to criminal and civil cases. The evidence produce in these cases may belong to Digital Records. Whenever any Digital Record is submitted as evidence in a court of law many sections of Indian Evidence Act comes into the picture.

Following are certain amendments made in the evidence act for the legal recognition of electronic records as evidence.

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872 (See section 92) [1 OF 1872]

1. IN SECTION 3,-

[128] André Årnes, 'Cybercrime Law', Published Online: 23 MAY 2017, DOI: 10.1002/9781119262442.ch3, Available at: <http://onlinelibrary.wiley.com/doi/10.1002/9781119262442.ch3/>

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the word "all document including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely :- the expressions; "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records". "Information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.

2. IN SECTION 17,

For the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. AFTER SECTION 22,

The following section shall be inserted, namely: - relevant. Oral admissions as to the contents of electronic records are not relevant unless the genuineness of the electronic record produced is in question."

4. IN SECTION 34,

For the words ***"Entries in the books of account",*** the words ***"Entries in the books of account, including those maintained in an electronic form"*** shall be substituted.

5. IN SECTION 35,

For the word ***"record"*** in both the places where it occurs, the words ***"record or an electronic record"*** shall be substituted.

6. FOR SECTION 39,

The following section shall be substituted, namely: - "39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or

papers.[129] When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made".[130]

7. AFTER SECTION 47,

The following sections shall be inserted, namely: - "47A.Opinion as to digital signature where relevant. When the Court has to form an opinion as to the digital signature or any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. IN SECTION 59,

For the words ***"contents of documents"*** the words ***"contents of documents or electronic records"*** shall be substituted.

9. AFTER SECTION 65,

The following sections shall be inserted, namely: - 65A.special provisions as to evidence relating to the electronic record. The contents of electronic records may be proved in accordance with the provisions of section 65B i.e., ***Admissibility of electronic records.***[131]

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further

[129]Caloyannides, Michael A, (2001), Computer Forensics and Privacy, Artech House <www.artechhouse.com>
[130] Casey, Eoghan (3rd Ed), Digital Evidence(Forensic Science, Computers & the Internet Computer Crime), Academic Press
[131]Justice Singh, Yatindra (2nd Ed), Cyber Laws, Universal Law Publishing Co Pvt Ltd

proof or production of the original, as evidence of any contents of the original or of any fact stated therein or which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer outputshall be the following, namely:-

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronicrecord or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purposes of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by a computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers. all the computers used for

that purpose during that period shall be treated for the purposes of this section as constituting a single computer, and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-

(a) identifying the electronic record containing the statement and describingthe manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied

thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to it is being stored or processed for the purposes of those activities by a computer-operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.- For the purposes of this section, any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process;

10. AFTER SECTION 67,

The following section shall be inserted, namely: - "67A. Proof as to digital signature. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved;"

11. AFTER SECTION 73,

The following section shall be inserted, namely: - "73A. Proofs as to verification of the digital signature. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by the person.

Explanation.- For the purpose of this section "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000.

12. AFTER SECTION 81,

The following section shall be inserted, namely:- "81A. Presumption as to Gazettes in electronic forms. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. AFTER SECTION 85,

The following sections shall be inserted, namely: - "85A. Presumption as to electronic agreements. The Court shall presume that every electronic record purporting to be an agreement containing the digital signature of the parties was so concluded by affixing the digital signature of the parties. 85B. Presumption as to electronic record and digital signatures.

(1) In any proceedings involving a secure electronic record, the Court shall presume unless the contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that

(a) the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to the authenticity and integrity of the electronic record or any digital signature. 85C. Presumption as to Digital Signature Certificates. The Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

14. AFTER SECTION 88,

The following section shall be inserted, namely:- 88A. Presumption as to electronic messages. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission, but the Court shall not make any presumption as to the person by whom such message was sent. Explanation.- For the purposes of this section, the expressions ***"addressee"*** and ***"originator"*** shall have the same meanings respectively assigned to them in clause (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000;

15. AFTER SECTION 90,

The following section shall be inserted, namely: - "90A. Presumption as to electronic records five-year-old. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular was so affixed by him or any person authorised by him in this behalf.[132]

Explanation.- Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to section 81A."

16. FOR SECTION 131,

The following section shall be substituted, namely: - "131. Production of documents or electronic records which another person, having possession, could refuse to produce. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control unless such last-mentioned person consents to their production."

1.5 EVIDENTIARY VALUE OF ELECTRONIC RECORDS

The evidentiary value of an electronic record is directly proportional to its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records.[133] According to section 3 of the Act, “evidence” means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence. Thus the section clarifies that documentary evidence can be in the form of electronic record and stands at par with the conventional form of documents.

The evidentiary value of electronic records is elaborated under sections 65A and 65B of the Evidence Act, 1872. These sections provide that if the four conditions listed are satisfied

[132]Submitting an Email or Electronic Record <https://lawgic.info/submitting-an-email-or-electronic-record-as-evidence-in-an-indian-court/>

[133]Cyber Forensics & Electronic Evidences: Challenges <http://www.legalservicesindia.com/article/975/Cyber-Forensics-&-Electronic-Evidences:-Challenges-In-Enforcement-&-Their-Admissibility.html>

any information contained in an electronic record which is printed on paper, stored, recorded or copied in an optical or magnetic media, produced by a computer is deemed to be a document and becomes admissible in proceedings without further proof or production of the original, as evidence of any contacts of the original or any facts stated therein, which direct evidence would be admissible.

1.6 LET'S SUM UP

In this chapter, we have studied the relevance of Indian laws to cyber forensics along with the amendments that took place in the Indian Evidence Act with respect to Electronic evidence. Finally, we ended the discussion with the evidentiary value of electronic records.

1.7 FURTHER READING

- Rodriguez, Glen & Molina, Fernando. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics. 9. 1. 10.1504/IJESDF.2017.10002624.
- Medcraveonline.com (2019), http://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf (last visited Nov 26, 2019).
- https://www.ncjrs.gov/pdffiles1/nij/211314.pdf
- https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How does evidence help in a case?**

With the help of evidence, facts related to the incident are established at trial. Indian Evidence Act contains a set of rule and related issues governing the admissibility of evidence in the Indian Courts of Law.

2. **What are the 2 divided categories of the provisions of Evidence Act?**

The Evidence Act provisions can be divided into 2 categories:

- Taking the evidence (By Port) - This means to take the evidence for the facts. The fact means the things which are said before the court in connection with the matter. These facts are given to the court either orally or documentary (also electronic documents).
- Evaluation – In evaluation court check whether the facts produce are capable to prove the evidence. Forensics plays a vital role in the evaluation phase.

3. What does the evidentiary value of electronic records mean?

The evidentiary value of an electronic record is directly proportional to its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records. According to section 3 of the Act, "evidence" means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence. Thus the section clarifies that documentary evidence can be in the form of electronic record and stands at par with the conventional form of documents.

1.9 ACTIVITY

Elucidate the amendments made in the Indian Evidence Act with respect to electronic evidence also briefly explain the admissibility of electronic records with relevant case laws? (1000 – 1500 words)

Unit 3: Cyber Forensics Labs and Challenges before Law Enforcement Agencies

3

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction to cyber forensic labs

1.3 Cyber forensic lab structure

1.4 Examiner of Electronic evidence

1.5 Introduction to Computer emergency response team India (CERT-In)

1.6 Objectives of CET-In

1.7 Challenges before law enforcement

1.8 Challenges while Investigation

1.9 Dark web (Dark net)

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The requirement for cyber forensics lab and how to build it.
- The details of examiner of electronic evidence by government of India.
- Computer Emergency Response Team India.
- Challenges before law enforcement agencies in India while investigation.
- Dark web and how Law enforcement deals with it.

1.2 INTRODUCTION TO CYBER FORENSIC LABS

Cyber Forensic lab is a facility where digital evidences are examined, analysed and the forensic report is been produced. There is a specific way to establish a cyber-forensic facility. Let's discuss certain points which are taken into consideration for setting up a cyber-forensic lab.

1.3 CYBER FORENSIC LAB STRUCTURE

- **LAB SPACE**

  The cyber forensic facility should be located at secured premises. The facility should not be congested and should have enough working space. There should be adequate and uninterrupted electricity. The forensic lab should have an effective cooling system without any humidity present inside the lab. There should be good internet connectivity at high speed. There should be enough desk and benches with the antistatic floor. There should be a lock for every room with an access control mechanism to prevent unauthorised access.[134]

- **REQUIRED EQUIPMENTS**

  There should be multiple hardware write blockers which supports all types of connectivity. E.g. SATA, Firewire, USB etc. There should be a high configuration computer system with the fastest speed of processing. There should be multiple good monitor. The forensic lab should have hardware filled kit. There should be enough blank hard disk and storage container which is called as evidence vault. There should be all sort of data and power cables with static bags. There should be enough supplies of packaging and labelling material. For network connectivity, there should be enough networking devices.

- **APPROPRIATE SOFTWARE**

  Forensic lab requires different types of software for different analysis purpose. There are a few examples like Encase, Accessdata FTK, Net force suit, Oxygen mobile forensic, Passware password recovery, Helix live CD etc.

[134] meity.gov.in. <https://meity.gov.in/writereaddata/files/annexure-i-pilot-scheme-for-notifying-examiner-of-electronic-evidence-under-section-79a-of-the-information-technology-act-2000.docx>

- **CYBER FORENSIC EXPERT**

  The cyber lab requires a team of cyber forensic expert with detailed knowledge of computing technology. These experts should be certified for the software and hardware installed in a forensic lab. These experts should have experience of expert witness testimony at court trials.

- **SOP(STANDARD OPERATING PROCEDURE)**

  There should be an established set of policies and procedures to be followed in a forensic lab for different purposes. E.g. wearing gloves before handling any evidence etc.

  There should be standard and approved format to prepare a chain of custody form. Examination notes, observation, finding and reports etc.

- **TRAINING AND UPGRADATION**

  To cop up with changing technology, the experts working with the forensic lab should undergo training every six months. The hardware and software used for the forensic examination should be upgraded as per requirement.

  The cyber forensic lab is a dedicated facility to carry out a forensic examination of digital evidence. These labs are mainly setup by government centrally and state wise.

1.4 EXAMINER OF ELECTRONIC EVIDENCE

The Information Technology Act, 2000 empowers the Central Government under section 79A to notify any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority specified by notification in the Official Gazette. The Explanation clause of section 79A further articulates that the “Electronic Form Evidence” means

any information of probative value that is either stored or transmitted in electronic form and includes evidence, digital data, digital video, cell phones, digital fax machine etc.[135]

a) In line with the above requirement, MeitY has formulated a scheme for notifying the Examiner of Electronic Evidence. The objective of the scheme is to ascertain the competence of all the desiring Central Government or a State Government agencies and to qualify them to act as Examiner of Electronic evidence as per their scope of approval through a formal accreditation process. Once notified, such Central, State Government agencies can act as the "Examiner of Electronic Evidences", and provide an expert opinion of digital evidence before any court.
The scheme is based on international standards like ISO/IEC 17025 (A Standard on General requirements for the competence of testing and calibration laboratories) and ISO/IEC 27037 (A Standard on Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence). The evaluation process includes an examination of the technical, skilled professional manpower in digital forensics, licensed tools and equipment, availability of suitable environment to carry out such evaluation as also the availability of a proper quality management system and reasonable experience to demonstrate their overall competency in this area.

Following is the listed lab of government as Examiner of Electronic Evidence

1. Cyber Forensic Laboratory, Army Cyber Group, DGMO, Signals Enclave, New Delhi
2. State Forensic Science Laboratory, Madiwala, Bangalore
3. Central Forensic Science Laboratory(CFSL), Hyderabad
4. Directorate of Forensic Science, Gandhi Nagar Gujarat
5. Computer Forensic and Data Mining Laboratory (CFDML), Serious Fraud Investigation Office (SFIO),
6. Notification of Forensic Science Laboratory Govt of NCT, Rohini New Delhi

1.5 INTRODUCTION TO COMPUTER EMERGENCY RESPONSE TEAM INDIA (CERT-In)

[135]The Impact of Technology on Organized Crime<https://www.sydneycriminallawyers.com.au/blog/the-impact-of-technology-on-organised-crime/>

CERT-In is a government body working under the ministry of electronics and information technology.It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur. As per the amendment in IT Act, CERTIN has been designated to serve the following functions in the area of cybersecurity as a national agency.[136]

- Collection analysis and examination of cyber incident.
- Forecast and alert cybersecurity incident.
- Co-ordination of cybersecurity responsibilities.
- Emergency measures for handling cybersecurity incidents.
- Issue guideline advisory, notes, whitepapers related to information security practices, procedures, preventions, response and reporting of cyber incidents.

CERTIN not only provides incident response services but also security quality management services. CERTs vision is to proactively contribute to securing cyberspace for India. CERTs mission to enhance the security of India's technology infrastructure through pro-active actions and effective collaborations. CERTIN has signed a memorandum of understanding with 7 countries of Shanghai Co-operation Organisation. With this MOU, participating countries can exchange technical information on cyber-attacks, incident response and solution to counter global cyber-attacks.

1.6 OBJECTIVES OF CERT-In

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

CERTIN function on 24 hours basis on all days of the year including government and other holidays. The contact details of CERTIN are published on website www.cert-in.org.in

[136]Nouh, Mariam & Nurse, Jason & Webb, Helena & Goldsmith, Michael (2019) Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement

Following are the types of cybersecurity incident need to be reported to CERTIN

- Targeted scanning of critical network systems.
- Compromise of critical system information.
- Unauthorized access to IT systems.
- Defacement of website or intrusion of the website.
- Malicious code attacks such as spreading virus, worm, Trojan, botnet, spyware etc.
- Attacks on the server such as database, mail and DNS.
- Identity theft, spoofing phishing attacks.
- Denial of service and distributed denial of service attacks.
- Attack on critical infrastructure, SCADA systems and wireless networks.
- Attacks on applications such as e-commerce and e-governance.

1.7 CHALLENGES BEFORE LAW ENFORCEMENT AGENCIES

As technology has brought lots of many changes into every organization, Law enforcement agencies (LEA) are not the exception for it.[137] Many LEAs are going under transformation and still in the adoption phase for this technological advancements. Make in India and Digital India is the current era for our country. But we are still in the process of replacing traditional ways while these positive changes around us. This has created a crucial challenge in the field of investigations as well. Let's understand the real situation and challenges faced by LEA in this digital era.

1.8 CHALLENGES WHILE INVESTIGATION

Due to the use of technology by criminals in their act the speed of execution of any crime has increased a lot.[138] LEA has to compete with the speed of the fraudster. Criminals are real users of advanced technology and find out many new technological ways to commit crimes. LEA's challenges start from understanding the use of technology by criminals in the given scenario.

[137] S W Brenner Cybercrime: Criminal Threats from Cyberspace, 2nd Edition. Praeger Security International. ABC-CLIO, LLC, 2018

[138] Hunton, PaulManaging the technical resource capability of cybercrime investigation.A UK law enforcement perspective. Public Money &Management, 32(3):225–232, 2012

Let’s divide the changes faced by LEA into 3 categories:-

1) ***Pre Investigation***

a) Not clear Understanding of the Jurisdictions:-

Due to jurisdictional issues of the cyberspace, many Investigation officers are not clear about who should investigate the scenario which involves different geographically distant location. For example, Person who is living in Bangalore who is over business trip in Pune receives the SMS which says his debit card is used in Delhi and his bank belongs to Chennai. Such a Situation confuse the Investigation officer that which state investigation agency is the right authority to investigate the given situation.

b) Lack of technological background

Nowadays, Criminals are using technology not only in cybercrimes but also in traditional crimes.IO are mainly Police Inspectors which may not be from a technical background. It becomes very difficult for them to understand the overall situation and that’s why it affects the speed of execution

2) ***During Investigation***

A. Lack of technological expertise
B. Availability of the required equipment’s
C. Absence of standard operating procedures for investigation
D. In Adequate expert witness

3) ***During Court trials***

- Cross border investigation
- Admissibility of electronic evidence
- Hash Value calculation

One challenge computer investigators face is that while computer crimes know no borders, laws do. What's illegal in one country may not be in another. Moreover, there are no standardized

nternational rules regarding the collection of computer evidence. Some countries are trying to change that. [139]

1.9 DARK WEB (DARKNET)

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view.In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

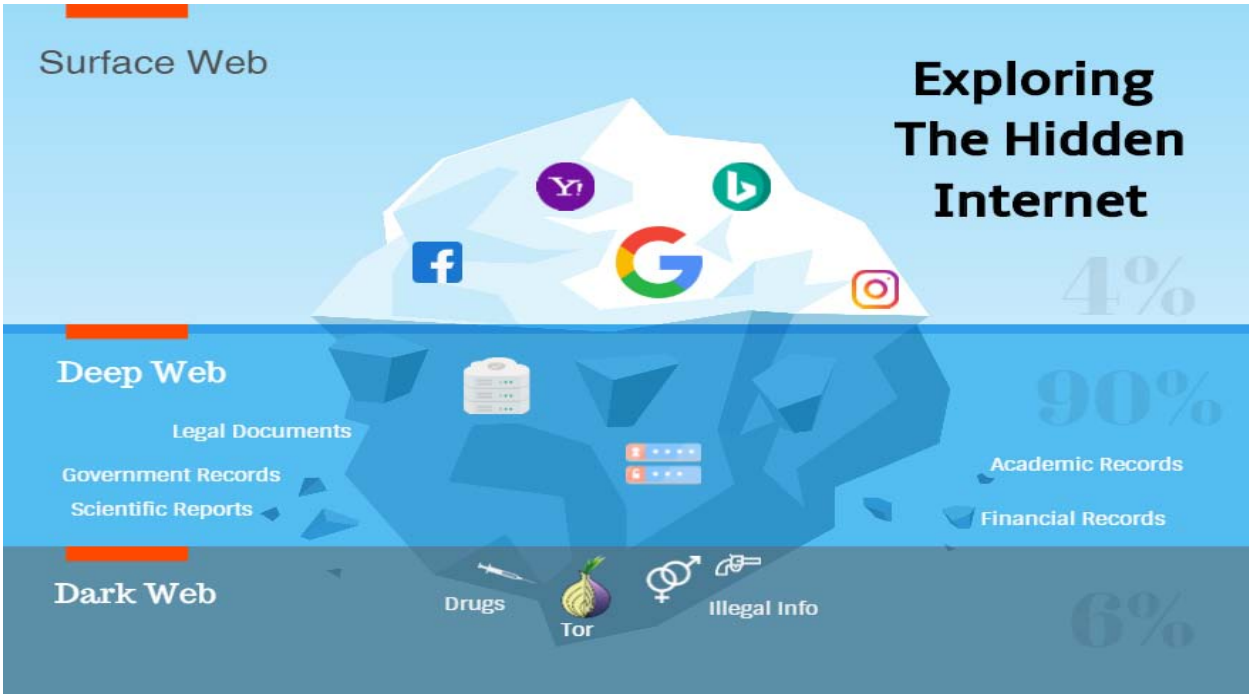


Figure 4.1:- The Internet is like an iceberg where most of the people can see only the surface and majority of the portion stays hidden.

The World Wide Web is considered as an iceberg, in which the regular sites that common people visit isthe top layer of the iceberg. This includes common sites such as Wikipedia, Google and

[139] Scott R Senjo An analysis of computer-related crime: Comparing police officer perceptions with empirical data. Security Journal, 17(2):55–71, 2004

even the millions of blogs that come and go daily. This portion is just 4% of the overall internet is known as surface web.[140]

Then it comes the portion of the deep web in which personal records, government documents and confidential information which are not meant for public view and are understandably kept safe. This information forms an ecosystem for many surface web applications. Hence, they are many times directly connected to the surface web. In order to dive into the Deep web pages one has to know that URL beforehand.[141]

The dark web is the underworld of the internet. It is the subsection of the deep web. But if anyone who is seeking access to Dark web pages, requires special software with the correct decryption key, as well as access rights and knowledge of where to find the content. The Dark Web is slightly more complicated because most of the times it runs on networks of the private servers, allowing communication only via specific means. This enables a high degree of anonymity and makes it difficult for authorities to shut down or monitor it.

If a cyber-attacker hacks into your organization and exfiltrates valuable business information such as customer records, or a disgruntled insider decides to try and sell some stolen intellectual property, they will simply prefer the dark web.

Unfortunately, the highest amount of anonymity and privacy has led to Dark Web to become a place where many illegal activities take place.[142]

DARK WEB BROWSER

Accessing the dark web requires the use of an anonymizing browser which is called Tor. It is free software that users download from the Internet to anonymously access the dark web.

Thousands of volunteers around the globe host and operate series of proxy servers through which tor browser routes the webpage request, rendering the real IP address unidentifiable and untraceable.

---

[140] Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper Series: No 6, February 2015, p 1

[141] Verisign, The Domain Name Industry in Brief, Volume 13, Issue 3, September 2016. A top-level domain is one at the top of the Internet's domain name system (DNS) hierarchy. For instance, the top-level domain is .com

[142] Stephanie Pappas, "How Big Is the Internet, Really?," Live Science, February 18, 2016

This process works well for the anonymity and privacy of the user, the Tor browser experience is typically unreliable and slow. One does not have direct control over his surfing because it is routed through different server hence use of credential seems to be unreliable via such service.

DARK WEB WEBSITES

The websites which are hosted over the surface web have ended in .com or other common suffixes, but the dark web URLs typically end in .onion which is a special-use domain suffix. Dark web sites are not easy to remember as well because of its URLs are a mix of letters and numbers. For example, one of the most infamous dark web marketplaces was the Silk Road, best known for selling illegal drugs that was eventually busted by the FBI which went by the URLs silkroad6ownowfk.onion and silkroad7rn2puhj.onion.

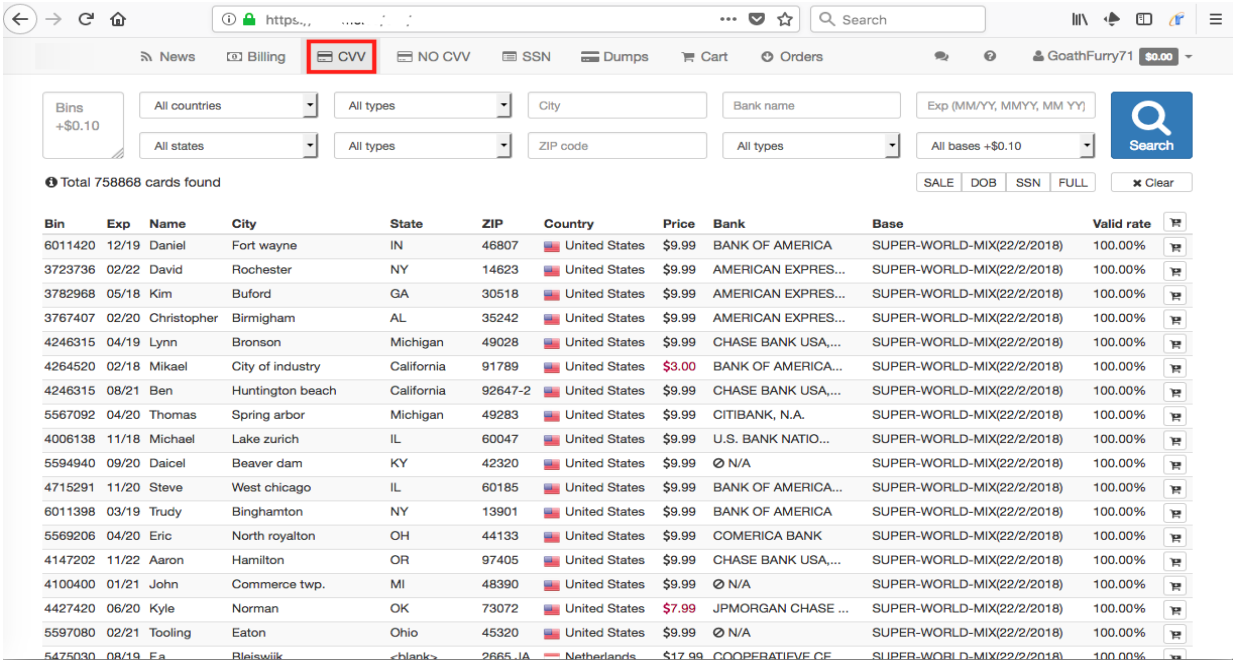
WHAT YOU CAN DO AT DARKNET?

As darknet is famous for anonymous surfing one can buy credit card numbers, all types of drugs, guns, counterfeit money, stolen subscription credentials, hacked subscription like Netflix accounts and software that is created and used by criminals to break into someone's computer. One can buy login credentials to a $50,000 Bank of America account for $500 or get $3,000 in counterfeit $20 bills for $600. One can buy illegal drugs with express shipping included in it. One can hire a hacker to attack computers for you. One can buy a lifetime subscription for Netflix account or pornographic websites just for 6$. One can buy usernames and passwords of business rivals.[143]

Hence, more legitimate companies are beginning to have a presence on the dark web. The cryptocurrency is very much useful for the users who can purchase anything on the dark web without revealing their identity.

Darknet acts as freedom which is given at large to do whatever you want without being identified. This thing provokes the criminal intentions of the person to strongly come out and to be followed by one.

[143] Andy Greenberg, "An Interview with Darkside, Russia's Favorite Dark Web Drug Lord," Wired.com, December 4, 2014



Bin	Exp	Name	City	State	ZIP	Country	Price	Bank	Base	Valid rate
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
3723736	02/22	David	Rochester	NY	14623	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3782968	05/18	Kim	Buford	GA	30518	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
3767407	02/20	Christopher	Birmigham	AL	35242	United States	$9.99	AMERICAN EXPRES...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4264520	02/18	Mikael	City of industry	California	91789	United States	$3.00	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	$9.99	CITIBANK, N.A.	SUPER-WORLD-MIX(22/2/2018)	100.00%
4006138	11/18	Michael	Lake zurich	IL	60047	United States	$9.99	U.S. BANK NATIO...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5594940	09/20	Daicel	Beaver dam	KY	42320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4715291	11/20	Steve	West chicago	IL	60185	United States	$9.99	BANK OF AMERICA...	SUPER-WORLD-MIX(22/2/2018)	100.00%
6011398	03/19	Trudy	Binghamton	NY	13901	United States	$9.99	BANK OF AMERICA	SUPER-WORLD-MIX(22/2/2018)	100.00%
5569206	04/20	Eric	North royalton	OH	44133	United States	$9.99	COMERICA BANK	SUPER-WORLD-MIX(22/2/2018)	100.00%
4147202	11/22	Aaron	Hamilton	OR	97405	United States	$9.99	CHASE BANK USA,...	SUPER-WORLD-MIX(22/2/2018)	100.00%
4100400	01/21	John	Commerce twp.	MI	48390	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
4427420	06/20	Kyle	Norman	OK	73072	United States	$7.99	JPMORGAN CHASE ...	SUPER-WORLD-MIX(22/2/2018)	100.00%
5597080	02/21	Tooling	Eaton	Ohio	45320	United States	$9.99	⊘ N/A	SUPER-WORLD-MIX(22/2/2018)	100.00%
5475030	08/19	Ea	Bleiswijk	<blank>	2665 JA	Netherlands	$17.99	COOPERATIEVE CE	SUPER-WORLD-MIX(22/2/2018)	100.00%

Figure 4.2:- stolen card details are sold in the underground market on the Internet.

DARKNET USERS

Out of the billions of internet users accessing the internet on an everyday basis, Dark Web use remains around 3 percent. Because of the nature of stuff over the dark web, one can easily understand that the dark web is mainly used by criminals, terrorist and activist but that is not the only case.[144]

The ethical use of the dark web is done by law enforcement or threat intelligence agencies. Security professionals may search through the dark web for signs of security or data breaches, evidence of illegal activity or newly emerging cyber threats. The dark web also hosts a large amount of educational information that cannot be found elsewhere, such as banned books, collections of news articles and discussion forums.

DANGERS OF THE DARK WEB

[144]Beshiri, Arbër&Susuri, Arsim (2019) Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications.

Accessing the dark web and using the tools or services found there, can be associated with high risks for an individual user or an enterprise. A few dangers that users should be aware of before browsing the dark web includes:

- Unknown Infection of viruses or malware especially ransomware,
- Installation of spyware such as key loggers.
- Infection of the system with Remote access tools (RAT) with new signatures.
- Distributed denial of service (DDoS) attacks.
- Identity theft, credential theft or phishing.
- Compromise of personal, customer, financial or operational data.
- Leaks of your own intellectual property or trade secrets.
- Spying, webcam hijacking or cyberespionage.

DARK WEB FROM LAW ENFORCEMENT VIEW POINT

Use of the dark web brings in unique challenges for law enforcement agencies in India. The law enforcement officer feels that if there were some police presence on the dark web, they will be in a better position to deal with the possible attack. Cyber experts say that some officers go undercover on the dark web to keep track of illegal activities going on there. That monitoring the dark web can help to boost cybersecurity, identify breaches and vulnerabilities. An officer said that prior to the Cosmos Bank fraud in Pune in which Rs 94 crore was fraudulently transferred from the bank, there was chatter on the dark web about people looking for details on Indian banks. This shows the Indian LEA officers mainly believes gathering evidence on the dark web activity is comparatively difficult but not impossible.[145]

In order to combat with such highly technical types of criminal activities, there is a need for police officers to be trained in changing cyber trends who are dedicated only to cyber-crime and not transferred to other police units. Hence, this leaves us with the hope that the expert criminals

[145]Dilipraj, E (2014) Terror in the Deep and Dark Web. 9. 121-140

cannot permanently hide in places like darknet and they are under radar even they stay in this underworld of the internet.

1.10 LET'S SUM UP

In this chapter, we have studied about the cyber forensic labs and the structure of it. We also studied about Computer emergency response team India and its objectives. Finally, we ended the discussion with the Dark web and challenges while investigation.

1.11 FURTHER READING

- Saran, Vaibhav& A.K.GUPTA,. (2014). Cyber Crime & Their Forensic Investigation.
- Yeboah-Boateng, Ezer&Akwa-Bonsu, Elvis. (2016). Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber-crimes. Journal of Cyber Security and Mobility. 4. 87-104. 10.13052/jcsm2245-1439.425.
- Ficci.in (2019), http://ficci.in/spdocument/22982/FICCI%20-%20EY%20Report%20-%20Confronting%20the%20New%20Age%20Cyber%20Criminal.pdf (last visited Nov 27, 2019).
- Digitalcommons.law.scu.edu (2019), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1219&context=scujil (last visited Nov 27, 2019).

1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Summarize about cyber forensic lab structure?**

- Lab Space
- Required Equipments
- Appropriate Software
- Cyber Forensic Expert

- SOP(Standard Operating Procedure)
- Training and upgradation

2. What is CERT-In?

CERT-In is a government body working under the ministry of electronics and information technology.It is operational since 2004. CERT-In is a national nodal industry responding to the computer security incident as and when they occur.

3. What are the objectives of CERT-In?

- Preventing cyber-attacks against the country's cyberspace.
- Enhancing security awareness among common citizen.
- Responding to cyber-attacks and minimizing the damage as well as recovery time.

4. What is the Dark Web?

The dark web, which is also called a darknet, is an encrypted portion of the internet which cannot be indexed by search engines. It is purposefully created portion of the internet which is not for public view.In order to access the dark web, the special anonymous browser is used. Websites on the dark web have an unconventional naming structure. Hence, anyone who wants to access such websites needs to know them in advance.

1.13 ACTIVITY

Briefly explain what is dark web, how it is being used and the dangers pertaining to it? Elucidate the illicit activities that has been taking place via the dark web with a case study? (1000 words)

Unit 4: Mobile Network Investigations

4

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Mobile Network Technology
1.4 Investigations of Mobile Systems
1.5 Types of evidence
1.6 How data may be acquired
1.7 Let's sum up
1.8 Further reading
1.9 Check your progress: Possible answers
1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Mobile Network Technology
- Types of evidence
- How data may be acquired

1.2 INTRODUCTION

The use of mobile devices is increasing rapidly, with devices like the BlackBerry, iPhone, and G1 providing a wide variety of services, including communication (e.g., voice, SMS, e-mail), Internet access (web browsing), and satellite navigation (GPS). These technological advances

create new opportunities for criminals while providing valuable sources of evidence. The bombs in the 2004 train bombings in Madrid apparently used cellular telephones as timers. The terrorists in the recent Mumbai attacks communicated using satellite telephones. Drug dealers and organized criminals are heavily dependent on inexpensive prepaid cellular telephones that are essentially anonymous and disposable.[146]

Mobile network investigations are also commonly performed for "conventional crimes," often focusing on location information, logs of telephone calls, printouts of SMS messages, and associated metadata.A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

1.3 MOBILE NETWORK TECHNOLOGY

In the late 1980s, the mobile telephony system in Europe was based exclusively on the ETACS network created by various telephone companies and consisting of analog radio links operating at the frequency of 800 MHz. Although at the time it was considered to be the start of a revolution, few would have imagined how quickly the phenomenon would burgeon both into a fad and into a system for keeping close track of individuals.

The weak points of the ETACS network were the lack of coverage abroad, continuing interference with other users, and the ease of cloning. It often happened that some unknown party obtained possession of the serial number of a mobile device, combined it with a new account to elude the NSP and generated telephone traffic paid for by the unwitting victim. In the mid-1990s, the GSM network was introduced. It operated at a frequency of 900 MHz and later 1.8 GHz. GSM was introduced precisely to eliminate once and for all the problem of interference among radio links and, being digital, to make conversations more secure.[147]

The next revolution in mobile network technology came about in 2003 when the Japanese colossus Hutchinson Whampoa entered the European market with H3G, the third generation of mobile telephony. The telephone now became a video-telephone, using the 2.1 GHz band.In the

[146] Curran, Kevin & Robinson, Andrew &Peacocke, Stephen & Cassidy, Sean (2010) Mobile Phone Forensic Analysis
[147](Bucks.edu, 2020)
<https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf>

area of electronic communication services, it is necessary to distinguish between "telephony" and "telematic" services.

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice messaging, conference calls, and data transmitted via telefax.	Internet access, E-mail.
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

A mobile device begins to leave its traces on the mobile network the moment it is turned on. When a device is powered on, it announces itself to the mobile network, generating a refresh of the authentication process. Like every technical device, a mobile device also releases technically sensitive information.[148] For example, an International Mobile Subscriber Identity (IMSI) is essentially a unique number that is associated with a particular subscriber on a GSM or UMTS mobile network. The IMSI is stored on the SIM card in a mobile device and is used to authenticate the device on the mobile networkand to control the other details such as HLR (Home Location Register) or copied locally in the VLR (Visitor Location Register). In order to avoid interception of this sensitive number, the IMSI is not directly sent over the network. It is substituted by a TMSI (Temporary Mobile Subscriber Identity), which is a temporary number, usually created for a single session. At the request of digital investigators, NSPs can use these unique identifiers to query their systems for all activities relating to a particular subscriber account.[149]

1.4 INVESTIGATIONS OF MOBILE SYSTEMS

Investigations used to be carried out exclusively by people. In the pure spirit of investigation, you started from information obtained through an undercover agent followed by operations

[148] ACPO (2009) Practice Guide for Computer-Based Electronic Evidence, (2009), <www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf>

[149] Gratzer,V, Naccache, D., Znaty, D (2006) Law Enforcement, Forensics and Mobile CommunicationsPerCom Workshop, Pisa - Italy, 13-17 March 2006, pp: 256-260

involving trailing suspects and intercepting ordinary mail. Without the help of technological systems, these investigations tended to last much longer than their more modern counterparts.[150]

Today, the initiation of an investigation may involve, in addition to verbal information, an anomalous bank record, an image from a surveillance camera, or of course highly visible crimes such as theft or murder.

The first phase of the investigation involves interviewing people who may have relevant information and continues with monitoring the means of communication of suspects or others associated in some way with the case. In addition to the traditional telephone, there are other monitoring points such as electronic mailboxes, places visited by the suspect, Telepass accounts (devices used for automatic highway toll payment), credit card accounts, and other financial operations.

Nowadays, investigations are supported by software that is customized to meet different requirements. The investigator enters all the data available on a subject into the interception system, and the server performs a thorough analysis, generating a series of connections via the mobile devices involved, the calls made or received, and so on, providing criminal police with a well-defined scheme on which to focus the investigation, and suggesting new hypotheses or avenues that might otherwise be hard to identify. Thanks to the support of the NSP, the data can be supplemented with historical information or other missing data such as other mobile devices connected to a given BTS on a given date and time. Data can also be provided for public payphones, which are often used to coordinate crimes. Again, thanks to a connection with the NSP, it ispossible to obtain a historical record of telephone calls made and the location of the payphone with respect to other mobile devices. The same sort of record may also be obtained for highway travel using Telepass (the conventional name for automatic wireless toll payment), including average speed and stops.[151]

Having historical data of various kinds relating to an investigation accessible in a database can greatly assist the initial examination of a newly acquired mobile device. By extracting all

[150]Harrill, D C, Mislan, R. P. (2007) A Small Scale Digital Device Forensics ontology, Small Scale Digital Device Forensics journal, Vol 1, No 1, June 2007

[151] McCarthy, P. (2005) Forensic Analysis of Mobile Phones <http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf>

telephone numbers in the phonebook of a mobile device seized during a search and entering names and numbers into the electronic system, digital investigators perform powerful analysis even in the initial phases of the investigation thanks to cross-referencing capabilities.

1.5 TYPES OF EVIDENCE

Mobile networks can provide information of relevance to an investigation, including the location of a mobile device, the past usage associated with a particular device or subscriber, as well as the context of communications.[152]

- ***Localization Parameters***

The term localization parameters describe the information that can be combined to localize an active mobile device and its related user. These localization parameters can be useful to track the position of a mobile device user, for several purposes, both for prosecution and defense.

- ***Determining the position of a given mobile device***

The simple act of turning on a device and leaving it in an idle state will generate data on the network that can be used to determine its approximate location. As a mobile device is moved from one location to another, it updates the network. Speaking, there is a timeframe where the mobile device "announces" itself to the network. The possible alternatives as follows:

a) Cell identification

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

b) Time difference of arrival (TDOA)

[152] McCarthy, P and Slay, J (2006) Mobile phones: admissibility of current forensic procedures for acquiring data. In Proceedings of the Second IFIP WG 11.9 International Conference on Digital Forensics, 2006

This method also referred to as multilateration, measures the time it takes for a signal to travel from a mobile device to multiple base stations to estimate the device location. “It is a method commonly used in civil and military surveillance applications to accurately locate an aircraft, vehicle or stationary emitter by measuring the time difference of arrival (TDOA) of a signal from the emitter at three or more receiver sites.”

c) Time of arrival (TOA)

This approach is effectively the same as TDOA, but this technology uses the absolute time of arrival at a certain base station rather than the difference between multiple stations.

d) Enhanced Observed Time Difference (E-OTD)

This method is similar to TDO, but in this case, the position is calculated by the mobile device, not the base station. In essence, the mobile device receives signals from multiple base stations at the same time that a specially placed receiver receives the signals. The precision of this method can vary from 50 to 200 m.

e) Assisted-GPS

A third-party service that generally relies on Cell Identification.

Determining the location of a mobile device can be important for assessing alibis of suspects or the whereabouts of victims in the past, and ongoing tracking of the location can be useful in cases of abduction, missing persons, and other ongoing criminal activities.[153]

From a practical perspective, there are tools that perform these techniques and display the results for digital investigators. Some of the information transmitted by the NSP to a monitoring centre is the position on the basis of cell and the IMSI code. This is extremely important information in that it makes it possible to track the people responsible for serious crimes as they move.

- ***Remote Activation of Electronic Devices***

Once, organized crime just used old-fashioned weapons. Now, with a mobile device and an Internet connection many more crimes can be committed. From the massacres of the 1990s to the latest terrorist attacks, mobile devices have played a fundamental role in the organization

[153] National Institute of Standards and Technology (2007) Guidelines on cell phone forensics, <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

ofcrimes. With a ring or an SMS containing a code, it is possible to activate or deactivate an electronic device in any part of the world. This is why the ability to trace an SMS or even a simple ring signal is particularly important, along with the refinement of technology for capturing any signal or use, even if innocuous, of mobile phones.[154]

Unfortunately, organized criminal groups, having considerable financial resources, enjoy various advantages in terms of budget and decision-making speed in undertaking countermeasures to thwart the various investigation and law-enforcement bodies. They hire experts in technology as well as researchers who spend their days seeking out the latest solutions in terms of protection.

When criminal figures meet for business, they often protect their privacy by jamming signals in the area around their meeting place. This prevents mobile devices from linking to the BTS and thus connecting to the network. This prevents investigators from connecting to the cell and getting an idea of the geographical location of the meeting. The jamming mechanism also temporarily interrupts the operation of mobile phones in the area that might represent a threat of interception.

A mobile device jamming system emits a signal to prevent the use of mobile phones within a certain radius. It emits a wideband radio signal at the same frequency range used for transmitting signals from the BTS to the mobile phones. This signal prevents the mobile device from decoding the network signal and thus causes the mobile device to disconnect from the network.

- ***Usage Logs/Billing Records***

The logs maintained by an NSP can help digital investigators determine past usage of a mobile device, as well as communications between individuals. These logs are generated from Call Detail Records (CDR) maintained for billingpurposes. The data in the resulting logs that are commonly provided to investigators are summarized here:

- Telephone number of user
- Numbers called
- IMEI number of mobile device

[154]Punja, S, Mislan, R (2008) Mobile Device Analysis, Small scale digital device forensics journal, Vol 2, No 1, pp: 1-16, June 2008, ISSN: 1941-6164

- Information about the cell: provides information about the location of the calling phone on the basis of the BTS where the connection was made
- SMS sent: excluding the text, which is available only via decodification using a telephone signal interception system.
- Date, time, and duration of calls

Depending on the equipment used, the logs generated on a particular mobile network may include a variety of other details.The Oracle Communications Services Gatekeeper is used by many NSPs world-wide for service delivery platform (SDP) infrastructure in a controlled, optimized, and automated way.Many external operators, including police units, have direct access to mobile network usage data via the Oracle Communications Services Gatekeeper solution, which is based on information technology, web and telecommunications industry standards such as Java Platform, Enterprise Edition (Java EE), web services, Session Initiation Protocol (SIP), IP Multimedia Sub-systems (IMS), Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Investigators will find this data interesting for their activity.

- ***Text/Multimedia Messages***

A common use of mobile devices is to send messages in text or multimedia format. The Short Message Service (SMS) communication service, which has been in use for some fifteen years, allows transmission of a limited number of text characters using the telephony channel. The advantages of the service include the possibility of transmitting messages even in areas of very low GSM signal coverage, where a voice call would be disturbed or fail due to insufficient signal strength, and even when the voice channel is being used for a conversation.

SMS messages are intercepted using the same systems as used for intercepting voice calls. These systems not only record the telephone numbers of the originator and the recipient but also the entire text of the message. On some networks, the SMS messages are archived for extended periods.The Multimedia Message Service (MMS) is a more evolved form of SMS, where it is possible to attach other multimedia content to a classic text message, such as an audio, video, or photo file. Current interception systems also capture the multimedia content, saving it to a special folder for display or listening.

1.6 HOW DATA MAY BE ACQUIRED

Various laws have been enacted to define how traffic data retained by NSPs may be acquired. Therefore, it is essential for investigators to be familiar with the legislation in force in the country or jurisdiction in which they are operating. In certain countries, for example, the defendant's counsel or suspect's lawyer has the right to request directly from the NSP only those traffic data that refer to the "accounts registered in the name of the client."[155]

In other countries, on the other hand, there are authorities specifically assigned by law to identify measures for guaranteeing the rights of the parties involved in questions of telephone and telematic traffic data retention for detecting, investigating, and prosecuting crime. Precisely for this reason, anyone accessing or processing these data must adhere to certain principles:

- The legislated requirement to provide specific safeguards regarding the type and quantity of data to protect and the risks correlated with said protection. Providers are already required to prevent said risks by upholding common security obligations that go beyond merely the minimum measures required by law or regulation. These risks are then assumed by those who receive the data.
- The advisability of identifying, given the current situation, protective measures to be implemented in the processing of data by all providers so that the integrity of said data can be verified in an inspection (and admissible in dealings with the suspect or defendant's counsel) to ensure more effective security for telephone and telematic traffic data.
- The need to keep in mind the costs deriving from the implementation of the measures in the various countries or jurisdictions, also regarding the different technical and financial capacities of the parties involved.
- The transnational legislative context, especially in light of the opinions expressed by the various groups working to protect personal privacy.
- The technological state of the art, meaning that the various measures have to be periodically updated.

[155]Willassen, S Y (2003) Forensics and the GSM mobile telephone system, International Journal of Digital Evidence, Spring 2003, Vol 2, No 1, pp:12-24

These are important matters with which to be familiar, especially in the field of cross-border investigations and litigation.[156]

1.7 LET'S SUM UP

In this chapter, we studied the technology-based investigations and acquisition of data with respect to it. We discussed the investigations of mobile systems and finally, ended the discussion with different types of evidence that would be collected via mobile systems.

1.8 FURTHER READING

- Gibbs, K. E., & Clark, D. F. (2001). In E. Casey (Ed.), Handbook of computer crime investigation. Academic Press.
- International Engineering Consortium. (2007). Time Division Multiple Access (TDMA). Available online at www.iec.org/online/tutorials/tdma/index.asp
- Prevelakis, V., &Spinellis, D. (2007). The Athens affair, IEEE spectrum. Available at www.spectrum.ieee.org/jul07/5280
- EDRI (2006). Telecom Italia wiretapping scandal. Available on EDRI Online, www.edri.org/edrigram/number4.15/italy

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) Define mobile device?

A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

2) Differentiate between Telephony and Telematic?

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice	Internet access, E-mail.

[156] Casey, E, Bann, M, & Doyle, J (2009) Introduction to windows mobile forensics. Digital Investigation, 6(3–4)

messaging, conference calls, and data transmitted via telefax.	
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

3) How is the cell identified in the process of investigation?

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

4) What is localization parameters?

The term localization parameters describe information that can be combined to localize an active mobile device and its related user.

1.10 ACTIVITY

Explain how the data is acquired through mobile device investigations along with how and what are the different types of evidence that are collected through the process? Briefly explain it with a relevant case study? (1000 words)

BAOU
Education for All

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

978-81-949119-2-0

BAOU
Education for All

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-201
Cyber Crime and Offences

Post Graduate Diploma in

Cyber Law

(PGDCL)

2021

Cyber Crime and Offences

Dr. Babasaheb Ambedkar Open University

Cyber Crime and Offences

Course Writer

Dr Peter Ladis	Chankaya National Law University, Patna, Bihar
Mr Kumar Gurav	Chankaya National Law University, Patna, Bihar

Content Reviewer

Dr Deesha Khaire	Gujarat National Law University, Gandhinagar

Content Editor

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr. Babasaheb Ambedkar Open University, Ahmedabad

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. 2021

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Cyber Crime and Offences

Block-1: Nature of Cyber Crimes

UNIT-1
Meaning and Definition of Cyber Crimes 02

UNIT-2
Classification of Crimes against Individuals 13

UNIT-3
Classification of Crimes affecting Economy 26

UNIT-4
Classification of Crimes against Society at Large 37

Block-2: Legislative Framework of Cybercrimes

UNIT-1
Legal Issues and Framework of Intercepting Wifi Transmission 49

UNIT-2
Cyber Security and International Legal Aspects 59

UNIT-3
Mapping the Costs of Cyber Crime 69

UNIT-4
Cyber Crimes: Global and Indian Response 78

Block-3: Types of Cyber Crimes

UNIT-1
Facets of Cyber Crime 90

UNIT-2
Cyber Terrorism 100

UNIT-3
Cyber Pornography 114

UNIT-4
Cyber Warfare 126

Block-4: International Law on Cyber Space

UNIT-1
International Law on Cyber Security in The Age Of Igital SovereIgnty 142

UNIT-2
The Customary International Law of Cyberspace 153

UNIT-3
Cyberwarfare and International Law 161

UNIT-4
International Courts for Cyberspace 171

Block-1

NATURE OF CYBER CRIMES

Unit 1: MEANING AND DEFINITION OF CYBER CRIMES

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Cyber Space and IT Evolution

1.4 History and Evolution of Cyber crimes

1.5 Definition of Cyber Crime

1.6 Nature and Scope of Cyber Crime

1.7 Doctrine of Mens Rea and Actus Reus in Cyber Crime

1.8 Characteristics of Cyber crime

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- History and Evolution of Cyber crime
- Nature and Scope of Cyber crime
- How doctrine of actus rea and mens rea play a role in cyber crimes

1.2 INTRODUCTION

Cyber crime is a collective term encompassing both ‘cyber contraventions’ and ‘cyber offences’. The word ‘cyber’ is synonymous with a computer, computer system or computer network. Thus, cyber crime may be defined as any illegal act that involves a computer, computer system or computer network, i.e., any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution.

In a broad context, cybercrime refers to any crime that includes a computer, computer network, mobile phone, or other electronic devices, either as a target or as a weapon or associate. As a consequence, any illegal activity carried out with or against such computer devices and in cyberspace is known as a cyber crime. The purpose or intention to inflict an accident, like all illegal acts, is one of the components, although it is not limited to any particular category. Stealing computer hardware is the beginning of illegal crime in the cyber world, and it leads to the conversion, modification, or loss of computer data in order to damage Internet users.

1.3 CYBER SPACE AND IT EVOLUTION

Crime isn’t a particular event that can be studied, interpreted, or represented in a single paper. It can be seen in every part of the world and in every social class. People of all ages, income classes, and backgrounds are among the perpetrators and victims. It’s impossible to say what’s going on with it. It has multiple causes. Its therapies are speculative and debatable. Computer-related offences, also known as cybercrime, are the most recent of all the crimes.

In 1984, William Gibson coined the phrase “cyber space” in his science fiction novel “Neuromancer.” Essentially, it refers to the interactive world in which computer operations take place. Cyberspace is a world without borders. It does not have any geographical borders.The geographical positioning of machines and people using

the internet has no effect on the internet address, making national boundaries irrelevant.The territorial limits of nations and the technological frontiers are unrelated. Since nations claim control over persons, activities, and happenings arising within their jurisdiction on the basis of geographical nexus, when territorial borders lose their significance, a well-established concept of international law is jeopardized. As a result, cyberspace contradicts the well-established concept of international law that citizenship and statehood are characteristics of authority over physical space and individuals.

Information technology is one of the world's fastest-growing markets. Rapid developments are emerging in the information technology sector as it moves from a control structure to one of liberalization and globalization. Knowledge is being regarded as a critical resource for country growth. The Indian government has taken a number of steps and interventions to implement effective automation in order to improve productivity and ensure the development of high-quality goods and services. The presence of qualified personnel is a plus factor. For the government, business, and industrial sectors, timely availability of credible, reliable, and coherent information on various accounts is crucial. Organizations in India are planning to face the burden of handling a changing world. To do this, processes and technologies must collaborate closely with the enterprise to include qualitative evidence at the required levels and at the right time for decision-making.Via the collection, organization, preservation, and distribution of information not only at the point of origin but also at various other relevant locations using appropriate communication infrastructure, information technology plays a significant role in this. In simple terms, the Internet is a global network of computers of various types, ranging from notebook computers to display computers, that connects 2 million computers across 13,300 networks to serve over 50 million users worldwide. The 'World Wide Web,' or digital superhighway, is another term for this. A 'Website' is a term used to describe each individual network on the internet.

1.4 HISTORY AND EVOLUTION OF CYBER CRIMES

All who uses palmtops and microchips today will be shocked to find that the first popular computer was installed in the 1950s, and the scale of the computer was so huge that it took up the whole space, and they were too costly to run. The use of these machines was inaccessible to a vast majority of people, and only a limited

number of specialists had extensive access to them and the expertise to operate them. At the turn of the twenty-first century, personal computers became more affordable and commonplace in India. After World War II, the US Department of Defense developed the Internet with the intention of developing a network that could operate in the event of a catastrophe or war and safely exchange information. ARPANET was the first network, and with the introduction of Transmission Control Protocol/Internet Protocol, the World Wide Web, and Hypertext, the internet became a global phenomenon. The accuracy and diversity of knowledge have improved as the Internet has risen in popularity. However, no one expected the possibilities that the internet would bring to tech-savvy offenders at the moment.

In India, the state-owned Videsh Sanchar Nigam Limited introduced internet services in 1995, and the government ended VSNL's monopoly in 1998, opening the sector to private operators. At the time, internet usage in India accounted for 0.1 percent of the total population; however, India has now surpassed China as the second-largest country in terms of internet access, with 33.22 percent of the population accessing the internet.

In common law systems, the mechanism of criminalizing individual conduct considered to be detrimental to the public generally takes time. Until undesirable acts are identified as "terrorism," traction acquired by issue detection and demands exercised by special interest organizations may easily cover decades. This mechanism can be exacerbated in certain cases by the emergence of such "catalyst events" that draw the public's and lawmakers' attention.[1]

In the year 1820, the first cybercrime was registered. That's not surprising given that the abacus, which is believed to be the oldest version of a device, has been used in India, Japan, and China since 3500 B.C. The era of modem machines, on the other hand, started with Charles Babbage's analytical engine. The loom was founded by Joseph-Marie Jacquard, a cloth maker in France, in 1820. This system required a series of steps in the weaving of special fabrics to be replicated. Employees at Jacquard became concerned that their traditional work and livelihoods would be jeopardized as a result of this.[2]

[1] Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.

[2] http://cybercrime.planetindia.net/intro.htm

Legislators became more concerned about computer crime in the 1980s as businesses became more focused on computers and as trigger incident cases revealed major vulnerabilities to computer crime violations. Criminals can also securely encrypt material that constitutes proof of their illegal activities, archive it, and even distribute it without fear of law enforcement detection. A cyber crime scene will now span from the regional point of victimization (e.g., the victim's personal computer) to every other point on the globe, further complicating police investigations.In effect, digital technology has significantly altered the criminal justice environment so that enterprising and opportunistic offenders have deliberately turned to the computer to perform their unlawful actions in circumstances where the device functions as the tool of the crime, the medium by which the crime is committed, as well as cases where the victim's computer, or computer system, is the victim's computer, or computer system.

As previously mentioned, the presence of modern computing technologies helps cyber criminals in cases where the device's function is incidental to the crime, such as when the machine is used to archive and secure information linking the perpetrator to illegal activities. The perpetrator, to a large extent, relies on the lack of technical capabilities in law enforcement to effectively execute the offences and escape undetected, which is a commonality in these types of crimes.Based on the analytical data available on investigators' self-assessed expertise in this field, computer offenders will have good cause to be confident about their chances of escaping capture.[3]

If we move closer to the twenty-first century, it will be clear that technological advances have opened the way for anyone who uses computer technologies today to enjoy modern and wonderful conveniences in their everyday lives, spanning from how to teach, shop, entertain, and develop a deeper understanding of market strategy and job flow.Our everyday lives have been permanently altered as a result of exponential developments in information technology. These advances allow us to interact over long distances in a matter of seconds and to collect and arrange vast volumes of data almost instantly, tasks that would otherwise be tedious and costly.However, the technical marvels that have enhanced the quality of our lives

[3] Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf

can be seen as a double-edged sword. Although computer technology has provided countless people with greater conveniences, it has also provided offenders with new opportunities.

1.5 DEFINITION OF CYBER CRIME

The Indian legislature has not specified cyber crime in any legislation, including the Information Technology Act of 2000, which deals with cyber crime. However, in general, the term "cybercrime" refers to any criminal action that is carried out over the internet or through the use of technology.

Cybercrimes are described by Dr Debarati Halder and Dr K. Jaishankar as "offences committed against persons or groups of individuals with a criminal purpose to deliberately damage the victim's identity or inflict physical or mental harm, or loss, to the victim directly or indirectly, using electronic telecommunication networks such as the Internet (chat rooms, emails, notice boards, and groups)".[4]

We don't have a clear description of cybercrime; however, the following are some general definitions:

"Criminal acts carried out by means of computers or the Internet," according to the Oxford Dictionary.[5]

"Those species of cyber crime whose genus is traditional crime and where the machine is either an object or target of the criminal conduct".[6]

"Any criminal or other offence encouraged by or requiring the use of electronic communications or computer systems, including any computer or the Internet, or either one or both of them" is classified as "cyber crime".[7]

Professor S.T. Vishwanathan had cited three definitions of Cybercrimes in his book *'The Indian Cyber Laws with Cyber Glossary'* which are as follows:-

- Any illegal activity in which a computer is a tool or object of the crime, i.e., any crime, the means or purpose of which is to influence the function of a computer.

[4] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed on 28th February, 2021)
[5] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 28th February, 2021)
[6] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 28th February, 2021)
[7] http://cybercrime.org.za/definition (Accessed on 28th February, 2021)

- Any incident associated with computer technology in which a victim suffered or could have suffered a loss; and a perpetrator, by intention, made or could have made a gain.
- Computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic transmission of data.[8]

1.6 NATURE AND SCOPE OF CYBER CRIME

Criminality is a psychologically mediated phenomenon. We will never be able to survive in a world without cybercrime, no matter how hard we try. In fact, if we haven't yet been able to get the crime rate down to a desirable level in the real world, how would we hope to do so in the virtual world, which is comparatively more unreal, infinite, and legally less controllable? However, the existence, scale, and meaning of crime in a particular society vary over time.The idea of a crime-free society is a fallacy, and crime cannot be isolated from society. As a consequence, the essence of a crime is dictated by the nature of a culture.

The complexity of a culture determines the complexity of the criminality that occurs in its environs. It is important and vital to check all of the causes that affect and lead to crime in order to comprehend crime in a society. The social and political institutions of society must grasp violence and the steps that can be taken to minimize it. When analyzing the nature and scope of a crime, the prevention and disciplinary steps taken by the machinery to control crime and criminal behaviour in society are not taken into account.

Technology advances have created new social and political issues in society, and rather than aiding the state in managing the crisis. They have created a new complicated scenario that is difficult to grasp and much more difficult to adapt existing legislation to. The state apparatus lacks the tools and expertise required to fight modern crime.

In the last three or four decades, computers have totally changed the human culture. It has not only made life simpler, but it has also significantly aided the physical, economic, and cultural integration of various parts of the world. Computer technology

[8] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81.

has allowed people to have access to information from all over the world when sitting in a room. Time and space barriers are no longer a problem due to new technologies. However, with the incredible benefits of using machines today, a jurisdictional problem has arisen in the legal system.

One component of transnational transactions over the internet that is difficult to assess is Jurisdiction. When courts were faced with questions of authority law, they were unable to determine the correct venue to hear lawsuits concerning cybercrime because the cyberspace or virtual universe became borderless when opposed to the real world, making it exceedingly difficult to monitor cybercrime.We are unable to solve the issue of cyber crime using local equipment because our machinery is incompatible with dealing with transnational crimes. Since cybercrime is so distinct from other forms of crime, the legislation in effect in the jurisdiction is inadequate to control it.

As a result, the global existence of cybercrime has made it impossible to control and fight. The advent of internet technology has provided us with many benefits, including the potential to cope with potential challenges and expand at an accelerated pace, but it has also provided offenders with the opportunity to commit crimes at the least amount of risk of detection. The internet has proven to be a boon to society's deviant actions. The idea of cybercrime has risen in importance, and we are now facing a major challenge from its impact on global culture. Because of our growing dependency on technology, human civilization is becoming more vulnerable to cybercrime.

Since cybercrime has become a worldwide epidemic, nationwide generalization of crime is no longer possible in the current situation. Our definition and enforcement of cybercrime must be regional, not global. Only by enacting new legislation and preparing global prevention and defence measures would we be able to protect our society from this evil known as "Cyber Crime".

As a result, the threat of cyber warfare/terrorism poses a significant threat to the planet and its institutions. Terrorism groups employ robotics to promote hate and attract militants, who are then trained using teaching tools. They're also introducing blogs and websites that teach them how to use arms and make bombs, among other things.

1.7 DOCTRINE OF MENS REA AND ACTUS REUS IN CYBER CRIME

Mens Rea and Actus Reus are the two most important concepts of conventional crime. "Such a consequence of human actions as the statute aims to prohibit," is defined as Actus Reus.[9] To be called a felony, there must be a commission or omission. Mens rea roughly refers to "a guilty state of mind."[10] The most significant aspect of crime is the mental component. The behavior remains the same, but the state of mind turns it into a*'reus'* and therefore an assault. About any crime necessitates the existence of a behavioural factor of some kind.[11]In the case of cybercrime, assessing the mens rea is exceedingly complicated.

In cybercrime, it's crucial to ascertain the hacker's mental state and whether or not the hacker was aware that the access was unauthorized. Thus, the hacker would not need to have intended to target a "Unique Device," as long as the unauthorized access was to "any computer." It gets easier for the hacker to show that he is an outsider with no power to enter because he is aware of the situation. However, where a hacker already has little authority, as in the case of a company executive, establishing that he violated his boundaries and was also aware of the fact that he was violating them becomes challenging.

Actus is the Latin term for "action." Since the entire act is performed in intangible contexts, reus in cybercrime has become a task. The suspect can leave any fingerprints in the machine itself, but demonstrating that in court would be a herculean task for the law enforcement apparatus, since it must be in actual shape or at least in a form that is admissible in testimony.[12]

1.8 CHARACTERISTICS OF CYBER CRIME

Cybercrime varies greatly from conventional crime in terms of definition. In comparison, as a result of the advent of Internet technologies, this activity has earned much more serious and unregulated exposure than typical crime. As a consequence, it is important to analyze the particular features of cybercrime.

---

[9] J.W.C. Turner, Kenney's Outlines of criminal law (19th Edition University Press, Cambridge 1966) 17. also at Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[10] R.C. Nigam, "Law of Crimes in India", Principals of criminal Law, Vol 1, (Asia Publishing House, 1965) 6.

[11] Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[12] Ibid.

- ***People with advanced expertise*** – Since cybercrime can only be conducted by technology, one must be highly knowledgeable about the internet, machines, and the internet in order to commit such a crime. People who conduct cybercrime are well-educated and have a detailed knowledge of how to manipulate the internet, making it impossible for police to apprehend them.
- ***Geographical problems*** – In cyberspace, there are no geographical borders. A cyber criminal can commit a crime in another part of the world while sitting in some part of the world. For example, a hacker in India might compromise a system in the United States.
- ***Digital Universe*** – The process of cybercrime takes place in cyberspace, but the perpetrator is physically situated outside of cyberspace. The criminal's entire activity when committing the crime takes place in the virtual universe.
- ***Collection of Evidence -*** Owing to the complexities of cyber fraud, collecting facts and prosecuting it before a court of law is exceedingly challenging. When committing cybercrime, the perpetrator invokes the jurisdiction of many nations while still hiding in a secure location where he cannot be identified.
- ***Unimaginable scale of violence***- Cybercrime has the capacity to cause injuries and death on an unimaginable scale. Cyberbullying, cyber pornography, and other crimes have a vast scope, and they can easily ruin websites and steal company records.

1.9 LET'S SUM UP

In this chapter, we have studied the evolution of cyber crime following how various authors have defined the term *'cyber crime'* as there isn't a clear definition under the Informaton Technology Act, 2000. We have also seen the scope of cyber crime in the present era along with how actus rea and mens rea play a pivotal role with respect to cyber crime. Finally, we ended the discussion with the different characteristics of cyber crime.

1.10 FURTHER READING

- S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81
- Rhiannon Williams, "The Biggest Ever Cyber Attacks and Security Breaches", The Telegraph, Available on http://www.telegraph.co.uk/technology/internet-security/10848707/The-biggestever-cyber-attacks-and-security breaches.html.

- See “Is Cyber-Terrorism the New Normal?” Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of cyber crime?**

The Indian legislature has not specified cyber crime in any legislation, including the Information Technology Act of 2000, which deals with cyber crime. However, in general, the term “cybercrime” refers to any criminal action that is carried out over the internet or through the use of technology.

2. **What is Actus rea and Mens rea?**

Mens Rea and Actus Reus are the two most important concepts of conventional crime. “Such a consequence of human actions as the statute aims to prohibit,” is defined as Actus Reus.To be called a felony, there must be a commission or omission. Mens rea roughly refers to “a guilty state of mind.”

3. **What are the different characteristics of cyber crime?**

Cybercrime varies greatly from conventional crime in terms of definition. In comparison, as a result of the advent of Internet technologies, this activity has earned much more serious and unregulated exposure than typical crime. The different characteristics of cyber crime are:

- People with advanced expertise
- Geographical problems
- Digital Universe
- Collection of Evidence
- Unimaginable scale of violence

1.12ACTIVITY

“Criminal activities in the cyber world are quite easier and most challengeable”- Explain the statement in the light of the Information Technology Act, 2000. (2000-2500 words)

Unit 2: CLASSIFICATION OF CRIMES AGAINST INDIVIDUALS

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Crimes affecting individuals

2.4 Invasion of Privacy

2.5 Law of Privacy: An Indian Perspective

2.6 Privacy in the Technology Driven World

2.7 Information Technology Act and Privacy

2.8 Voyeurism

2.9 Theft of Identity

2.10 Cyber Stalking

2.11 Let's sum up

2.12 Further reading

2.13 Check your progress: Possible answers

2.14 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of the crimes affecting individuals
- Privacy in the technology driven world and the IT Act
- Cyber Stalking

2.2 INTRODUCTION

The rapid strides in technological developments, especially in the fields of electronics and information technology, have heralded a new age in human life. However, technological innovations are not only helpful to humans; they also have detrimental implications. While technical advances such as telephones, cars, computers, cell phones, and other technologies have offered conveniences and other advantages, they have also provided new opportunities for offenders and wrongdoers. A significant number of young and misguided children are exploiting the internet and mobile phones for entertainment while causing a slew of problems for others, some of which are illegal in nature. Many offenders are also using machines as a means to promote illegal acts, such as theft, the selling or dissemination of child pornography, the sale of cocaine, and so forth. There is also systematic patent piracy and misuse of intellectual property rights.

The exponential development and application of the internet are transforming people's lives and supplying offenders with new methods of action. Criminals and criminals all over the world profit immensely from the Internet, e-mail, and other related technologies. The anonymity offered by modern networking modes such as e-mail, chat rooms, and other facets of the internet infrastructure helps offenders to work freely.Drug groups and jihadists all over the world now have new resources in the shape of these networks for organizing and extending their operations beyond their respective national boundaries. Criminals are even messing with the machine to see how they can use it in a different direction to carry out their crimes.

Criminals exploiting networks and information technology for nefarious ends have left all facets of human activity open to cybercriminals. For example, if a computer programmer is effective in changing a patient's medical order kept in a hospital's

computer, the patient's life could be jeopardized.A similar incident occurred in the United Kingdom, where the life of a 10-year-old child was put in peril. Cyber offenders are exchanging huge sums of money on a large scale. Frauds involving credit cards and ATMs are becoming more popular. People's anonymity has not been untouched. For e.g., when a senior television journalist went to withdraw money from an ATM in Delhi years ago, she wanted to get cozy with her male colleague. Their off-screen antics were filmed on the hidden camera and then shared in the offices of numerous TV stations.[13]The private video of Pamela Anderson and ex-husband Tommy Lee having sex was widely circulated online in another well-known Anderson Tape Cyber Scandal. These tapes are, without a doubt, the most popular stolen video of all time.[14] In dealing with the criminals operating in the evolution of criminality, law enforcement agencies and society must face new challenges.

2.3 CRIMES AFFECTING INDIVIDUALS

Of course, it is difficult to include a comprehensive and exhaustive list of the different kinds of illegal activity that occur in cyberspace because criminals are actively experimenting to discover new ways to commit crimes. The events in the cyber world are constant, and we are seeing a new form of cyber crime almost every day. Per contra, we will be discussing the different types of crimes affecting individuals in the present era. How the cyber crimes affect the individuals will then be very clear as most of them do affect the individuals too.

2.4 INVASION OF PRIVACY

Computers are the most significant means of protecting confidential and official records and personal knowledge in today's world. It helps you to store, manipulate, and transfer data even faster than any other concurrent record-keeping device. The Internet will now gather all sorts of information about a person that he might not be able to collect himself.When a person seeks medical attention in a hospital, for

[13] https://timesofindia.indiatimes.com/home/sunday-times/deep-focus/the-death-of-privacy/articleshow/991395.cms
[14]Ibid.

example, the hospital's machine receives his entire medical history and records. Similarly, a businessperson stores all details about his purchases in his machine.Any person who has access to this data, whether allowed or not, may use or misuse it.

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[15] Right to privacy is more of an implied obligation. It is the *'right to be let alone'.*[16] Right is an interest recognized and protected by moral or legal rules. It is an interest, the violation of which would be a legal wrong. Respect for such interest would be a legal duty. It is the basic principle of jurisprudence that every right has a correlative duty, and every duty has a correlative right. But the rule is not absolute. It is subject to certain exceptions in the sense that a person may have a right, but there may not be correlative duty. Nevertheless, it would be prudent if the issues related to privacy (and confidentiality) are viewed as *'right along with duties'.*

Allowing retained data to flow openly through the network carries the risk of jeopardizing an individual's life and safety, as well as a nation's protection. Individuals' right to privacy is recognized as a constitutional right in virtually every country. The availability of data in cyberspace, whether by hacking or other means of access, can result in a criminal invasion of privacy. It also infringes the right to privacy secured by Article 21 of the Indian Constitution.The Supreme Court has ruled clearly that the right to life requires the right to privacy.[17] Every person has a right to privacy, according to Article 12 of the United Nations Declaration of Human Rights.

Unsolicited requests from banks, telecom providers, and others for a deposit, credit card, or even a new connection, according to experts, led to "enemic violation of privacy of mobile telephony users at all times and hours" and significantly damaged citizens' constitutional rights.Personal data of subscribers is now commonly used by mobile service providers and telemarketers for commercial purposes as a product for sales marketing at the personal and financial expense of subscribers. Personal data provided by a subscriber to a cell telephone service company should be classified as private, and service providers should be forbidden from transmitting that data to other entities for commercial purposes by regulation.

---

[15] Westin, AF, Privacy and Freedom, 1967, London: Bodley Head.
[16] Warren and Brandeis 'The Right to Privacy' (1890) Harvard Law Review, IV (5).
[17] Mr. X Vs. Hospital 'Z' = 1988 AIR S.C.W. 3662; State of Maharashtra Vs. M.N. Mardikar, AIR 1991, SC 207; People's Union for Civil Liberties, V. Union of India; Kharak Singh Vs. State of U.P., 1964, ISCR, 332.

2.5 LAW OF PRIVACY: AN INDIAN PERSPECTIVE

Though the Indian Constitution has not guaranteed the right to privacy as a fundamental right to the citizens but nevertheless, the Supreme Court has come to the rescue of a common citizen, time and again, by construing *'right to privacy'* as a part of the right to *'protection of life and personal liberty'.* The right to privacy could be read into Article 21, which states that *'no person shall be deprived of his life or personal liberty except according to procedures established by law'.* In this context of personal liberty, the Supreme Court has observed that *'those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of law'.*[18]

In the case of *State vs Charulatha Joshi,*[19]the Supreme court recognized privacy rights and held that *'the constitutional right to freedom of speech and expression conferred by Article 19(1)(a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed, and no court can pass any order if the person to be interviewed expressed his unwillingness'.*

In *People's Union for Civil Liberties (PUCL) vs Union of India,*[20]the Supreme Court held that the telephone tapping by Government under Section 5(2) of the Telegraph Act amounts infraction of Article 21. Right to privacy is a part of the Indian Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed *'except according to the procedure established by law'.*

In *Ram Jethmalani vs Union of India,*[21] the Supreme Court had dealt with the right to privacy elaborately and held as under:

'Right to privacy is an integral part of right to life. This is a cherished constitutional value, and it is important that human beings should be allowed domains of freedom that are free of public scrutiny unless they act in a lawful manner. The solution for the problem of abrogation of one zone of constitutional values cannot be the creation of another zone of abrogation of constitutional values. The notion of fundamental rights,

[18] Ram Narain v. State of Bombay, 1952 SCR 652: AIR 1959 SC 459: 1959 SCJ 679.
[19] State v. Charulatha Joshi, (1999) 4 SCC 65; See also Prabhu Dutt v. Union of India, AIR 1982 SC 6; Sheela Barse v. State of Maharashtra, (1987) 4 SCC 373.
[20] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[21] Ram Jethmalani v. Union of India, (2011) 8 SCC 1.

such as a right to privacy as part of right to life, is not merely that the State is enjoined from derogating from them. It also includes the responsibility of the State to uphold them against the actions of others in the society, even in the context of the exercise of fundamental rights by those others'.

2.6 PRIVACY IN THE TECHNOLOGY DRIVEN WORLD

Privacy in the technology-driven world is a difficult proposition. Technology has become a kind of double-edged sword. On the one hand, it quips the person to safeguard his privacy, and on the other, it helps in blowing the privacy cover one may have had.

There are means to capture the digital footprints of the user (customer), who is browsing the Internet for various personal reasons. It all begins with capturing the Internet Protocol (IP) address. It is a kind of *personally identifiable information* that is automatically captured by another computer when any communications that is automatically captured by another computer when any communications link is made over the Internet. The computer resource in use could easily be identified as it has been given a unique IP address (static or dynamic) by the Internet Service Provider (ISP). Whenever a person browses, visits a site, sends an e-mail or chats online, he leaves his distinctive IP address behind. It is possible either by searching IP registration databases or by conducting a traceroute to determine an approximate physical location of an IP address.

2.7 INFORMATION TECHNOLOGY ACT AND PRIVACY

Regrettably, Indian laws are essentially vague on the issue of privacy rights. Even the Indian Information Technology Act of 2000, which was passed to "provide legal recognition for transactions carried out by way of electronic data exchange and other means of electronic communication," lacks sufficient protections to protect the right to privacy.However, section 72 of the Act provides a provision for punishment for violation/breach of confidentiality and privacy in the restricted sense of any person unlawfully and without the permission of the person concerned revealing any

electronic record, book, log, correspondence, records, papers, or other material to which he had access under any of the provisions of the Act.

Section 72 has a limited application only. It confines itself to the acts and omissions of those persons who have been conferred powers under this Act, rules or regulations made thereunder. The ides behind the said provision is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the disclosing party. An obligation of confidence arises between the *'data collectors/data controller'* and a *'data subject'.* In case of unauthorized disclosure of such information, the said person shall be punished with imprisonment for a term, which may extend to two years, or with fine, which may extend to one lakh rupees, or with both.

Besides Section 72 of the Act, there is a clause under section 74 of the Act that specifies that anyone who intentionally produces, publishes, or otherwise makes available a Digital Signature Certificate for some fraudulent or unlawful intent shall be punished with imprisonment of up to two years, a fine of up to one lakh rupees, or both.

In furtherance, Section 72A has been inserted by the new amendment act, which talks about punishment for disclosure of information in breach of lawful contract. This provision creates liabilities for service providers, including an intermediary. It is in fact, a kind of data protection measure, wherein a service provider who has secured access to any material containing personal information about a person, discloses such information without the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain to such a person.

Here, the issue of confidentiality and privacy as enumerated in Sections 72 and 72A of the IT Act should be read along with the reasonable restrictions imposed by Article 19(2) on right to *'freedom of speech and expression'* as enunciated in Article 19(1)(a) of the Constitution of India.

The Organization for Economic Co-operation and Development (OECD) issued recommendations in 1980, advising countries all over the world to follow sound data privacy policies in order to escape unreasonable limitations or data flows through

borders.[22] In 1990, the United Nations adopted a series of guidelines for governing computerized data files.[23]

2.8 VOYEURISM

'Voyeurism' is described as "a sexual pervert's act who gains joy from secretly watching sexual acts?" 'Voyeur' is a term used to identify someone who has a morbid curiosity in other people's bodies or objects.The rules of Section 67 of the IT Act, 2000 and others do not extend to such heinous acts. There is a serious lacuna in the Indian Information Technology Act,2000 as it relates to the protection of privacy of individuals in the region.If the said provision is to be successfully invoked, the prosecutor must demonstrate that the accused's photos were released on the internetin the form of a CD or via the internet.

The right to privacy is implied in the Indian Constitution under Article 21, which states the universal right to life, as the Supreme Court of India first acknowledged in 1964. However, the decision only applies to the state and is covered under the Human Rights Act, which contributed to the creation of national and state human rights commissions. In the absence of a categorical clause, law enforcement authorities usually accept that cybercrime against women comes under the rules of the Information Technology Act of 2000, the Indecent Representation of Women (Prohibition) Act of 1987, and certain parts of the Indian Penal Code.

The provisions of section 67 of the IT Act deal with the printing, dissemination, or causing to be published of any obscene material. Its spectrum contains lascivious content, information that appeals to obscene desires, and information that has the power to deprive or degrade those who are likely to hear, see, or read it. Inconsistencies created by other rules are overridden by the IT Act. Section 292 of the Indian Penal Code, which governs the selling and dissemination of indecent material such as brochures and pamphlets, is another statute that tackles the issue. Conviction will result in a three-year sentence and a fine set by the court. The Indecent Representation of Women (Prohibition) Act, 1987 attempts to put an embargo to this trend of advertising, magazines, literature, drawing, figures, and

[22] Guidelines of OECD for protection of privacy and transborder flows of personal data, Paris, 1980
[23] UN General Assembly, Resolution No. 45/95, dated 14 December, 1990.

other means of speech. However, the maximum penalty is just two years imprisonment and a fine of Rs. 2000.

The 2013 criminal law amendments, inter alia many other provisions, has incorporated Section 354-C to the Indian Penal Code, 1860 with the definition of Voyeurism. Let us have a look at this provisiton:

> **Section 354-C: Voyeurism:** Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image1 shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.
>
> **Explanations**
>
> 1. For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.
> 2. Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

The existing provisions of Indian law, according to legal experts, are not adequate enough. They claim that new technology should be used for good, and that in situations where "human rights are infringed and unsuspecting people are filmed to appeal to voyeuristic interests of others," the legislation should include stringent punishments, such as imprisonment for both the cameraman and the seller. They further advocate an amendment to the IT Act, as it actually only requires ACPs or Deputy Superintendents of Police (DSPs) to prosecute those crimes. This restriction

is unfair since there is a lack of officers up to the rank of ACP or DSP, and hence such a rule restricts police personnel. However, after the 2013 Crminal Law Amendments, FIR can be filed now in the Police Station and the Procedures are as per the provisions of the Code of Criminal Procedure, 1973.

2.9 THEFT OF IDENTITY

The term “theft of identity” or “identity theft” applies to acts of deception, theft, forgery, misrepresentation of fact, and impersonation, among other things, that include the use of another person’s identifying details. It erodes customer trust in the legitimacy of commercial transactions and infringes on personal privacy. Identity fraud may involve items like having a credit card and taking out loans in someone else’s name.The hiring of an apartment, non-payment of bills, acquiring a cellular phone service, buying a car, taking out a home loan, and other forms of illegal activities fall into this group. A more extreme form of ‘identity fraud’ happens where a thief commits a robbery in a victim’s home and leaves a felony record behind. The internet has developed into a simple, low-cost, and successful way of accessing the identity of innocent victims.

SMS spoofing is a modern form of cybercrime that comes under the umbrella of identity theft. In this type of fraud, the perpetrator uses web-based tools to send a message from a device to an innocent person by specifying another person’s name in the form of his or her cell phone number. It seems to the receiver that the message was received by the victim himself.

Section 66C of the Information Technology Act, 2000 deals with punishment for identity theft. This provision is meant to protect the identity of a user in the online medium. The prime objective of this section is to protect the privacy of all or any online users, including their personal information or data.

The perspective of the said provision is not to merely protect the information residing in a computer resource but to protect the authentication details of any person in the form of electronic signatures (including digital signatures), passwords, PINs, biometric identifiers or any such other unique identification feature. The offence of *‘identity theft’* is completed when there is a dishonest or fraudulent downloading, copying or extraction of the electronic signature, password or any other unique identification feature of any other person. In other words, the moment personal

information is downloaded, copied or extracted of any person – dishonestly or fraudulently, *mens rea* comes into existence. Whether the offender makes use of such downloaded, copied or extracted personnel information will be the *actus reus* component of the crime. As per Section 66C of the Act, the offender shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to rupees one lakh.

2.10 CYBER STALKING

Stalking has long been a part of our history. It's an act ofstrutting stiffly or haughtily' or 'approaching someone undercover or without revealing one's name.' In our culture, telephone stalking, especially by children, is a widespread phenomenon. Initially, the stalking was dismissed as a mild case, with no need for state or congressional action.Minor infractions such as harassing phone calls, unnecessary gifts, excessive chasing, and so on were either ignored or dealt with by other legal provisions of law.

Cyber stalking is a form of stalking in which an electronic medium, such as the internet, is used to threaten or contact another person without their permission. The word "cyber stalking" refers to the use of electronic media as a stalking weapon, such as the internet, e-mail, SMS, MMS, and so on. Cyber stalking is typically anonymous and can be carried out by someone anywhere in the world. It does not pose a physical danger or inflict abuse.There are a number of stalking tactics that a person may use to intimidate others even though they do not share a geographical boundary. It can have a multitude of physical, mental, and psychological effects on the survivor, which can be debilitating in some situations. Since more people are using the internet in their everyday lives, the possibility of cyber stalking is on the rise.

While Indian law acknowledges cyber stalking, there is no clear legislation in place to resolve this issue. There are no clauses in the Information Technology Act of 2000 that fix cyber stalking, cyber bullying, or cyber harassment. It's a blatant mistake on the part of the administration. However, the Information Technology Amendment Act, 2008, directly addressed Cyber Stalking under Section 66A, i.e., Punishment for sending offensive messages through communication service, etc.However, critics argued that section 66A would be used as a mechanism to limit individual freedom of

speech and expression, in breach of India's Constitution's Article 19(1), and in 2015, the Supreme Court of India struck down Section 66A of the Information Technology Amendment Act 2008, in the case of *Shreya Singhal vs Union of India,*[24] arguing that it was "grossly misapplied by the authorities."

As a result, the Information Technology Amendment Act, 2008 does not address stalking directly. However, the problem is treated as an"invasion of an individual's privacy," rather than the regular cyber offences discussed in the IT Act 2008. Hence, Sections 72 and 72A of the Information Technology Amendment Act, 2008 are the most commonly used provisions in India for regulating cyber stalking.

2.11 LET'S SUM UP

In this chapter, we have studied the classification of crimes affecting individuals along with the significance of right to privacy and the constitutional aspects related to it. In furtherance, we have also seen an overview of the crimes affecting individuals such as voyeurism, identity theft, cyber stalking and the provisions pertaining to the same under IT Act.

2.12 FURTHER READING

- Yar, M. (2006). *Cybercrime and society*. SAGE Publications Ltd, https://www.doi.org/10.4135/9781446212196
- Paul Bocij. (2004). Cyber Stalking: Harassment in the Internet Age and How to protect your family
- John Q. Newman. (1999) Identity Theft: The Cybercrime of the Millennium
- Susan W. Brenner. (2010) Cybercrime: Criminal Threats from Cyberspace (Crime , Media, and Popular Culture)

2.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is Cyber Stalking?**

[24] Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73

Cyber stalking is a form of stalking in which an electronic medium, such as the internet, is used to threaten or contact another person without their permission. The word “cyber stalking” refers to the use of electronic media as a stalking weapon, such as the internet, e-mail, SMS, MMS, and so on.

2. **What is the meaning of Identity Theft?**

The term “theft of identity” or “identity theft” applies to acts of deception, theft, forgery, misrepresentation of fact, and impersonation, among other things, that include the use of another person’s identifying details.

3. **Which provision of IT Act protects voyeurism?**

Section 67 of the IT Act protects voyeurism. It deals with the printing, dissemination, or causing to be published of any obscene material. Its spectrum contains lascivious content, information that appeals to obscene desires, and information that has the power to deprive or degrade those who are likely to hear, see, or read it.

2.14 ACTIVITY

Discuss the procedure and safeguards provided under IT Act for crimes affecting individuals along with case laws? (2000 words)

Unit 3: CLASSIFICATION OF CRIMES AFFECTING ECONOMY

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Hacking

3.4 Kinds of Hackers

3.5 Legal Provisions under IT Act

3.6 Virus/Malicious Programmes

3.7 Computer Sabotage

3.8 Computer Fraud

3.9 Theft of Telecommunication Service and Mobile Cloning

3.10 Copyright Infringement and Software Piracy

3.11 Economic Espionage

3.12 Tax Evasion and Money Laundering

3.13 Cyber Squatting

3.14 Internet Marketing Fraud

3.15 Let's sum up

3.16 Further reading

3.17 Check your progress: Possible Answers

3.18 Activity

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of crimes affecting economy
- Different kinds of cybercrimes using the computer and Internet
- Legal provisions pertaining to it

3.2 INTRODUCTION

E-commerce is the use of the Internet for the purpose of industry and commerce growth. The widespread use of the internet for commerce and industry has aided the growth and advancement of emerging technology and communication networks. The speed and cost-effectiveness are the main benefits. Electronic shopping, also known as e-commerce, has made it possible for people to do business across national borders without having to worry about time or distance. These scientific advancements, however, are not without their drawbacks. Since such large sums of money are exchanged in e-commerce, suspects are likely to be drawn in. Criminals that are armed with advanced electronic gadgets have a lot of options when it comes to carrying out their illegal operations.Today, terrorists use malware to conduct acts of spying, cyber theft, data frauds, and vandalism on a wide scale.

3.3 HACKING

In general, the word “computer hacking” refers to the act of manipulating, vandalism, or spying in order to gain access to a computer device. After large-scale use of computer networks by government, military, and commercial organizations, cyber criminals realized the value of hacking.

The hacking strategy is based on the connectivity and security mechanism that a network or device uses in general. Hacking has historically been accomplished by the use of popular passwords, physical monitoring of the device, or confidence tricks. Following the introduction of the internet, modern hacking and computer manipulation devices have been created. The following are some of the most popular hacking techniques:

a) IP-spoofing

An individual uses this strategy to gain unauthorized access to computers or networks by impersonating an approved and trusted device within the infiltrated network. Modification of IP addresses in data packet headers sent to an incoming portion of the network's router is how it's achieved. The routers are unable to differentiate between data sent from the outside and data sent from within the network. At present, newer routers and firewalls also claim to defend against this kind of threat.

b) DNS-spoofing

The "Domain Name Service" (DNS) is a service that maps host names to IP addresses. The act of 'DNS-spoofing' is the development of a false hotsmask during the resolution of the internet. The name of the host must be resolved to its IP address for any internet connection, and this is achieved by connecting with a DNS-server, which holds the hotsmasks in databases. Hackers try to intercept contact and send bogus hostname mappings to the victim's device when performing DNS spoofing attacks. This is conveniently accomplished by using malicious site applets that the attacked user has downloaded. The user's contact can be rerouted and transmission data captured as soon as the applet is enabled.

c) Web Spoofing

'Web spoofing' is less difficult than IP and DNS spoofing, which take more advanced technical skills. It is based on an optical illusion in which characters in hyperlinks on web pages appear to make an address look legitimate but actually lead to a wrong web site.By changing the letter '0' in the address www.micrsoft.com, for example, a hacker may build an incorrect web site. The majority of users did not presume any malicious intent.

3.4 KINDS OF HACKERS

a) Scamps:

Hackers do so for pleasure and have no intention of harming anybody.

b) Pioneers:

These are mostly young men who are intrigued by innovative new technology and pursue them without really knowing what they would discover.

c) Vandals:

Such hackers do harm for no personal gain.

d) Explorers:

Breaking into a computer machine is normally a pleasurable experience for such hackers.

e) Addicts:

Such individuals are physically addicted to hacking and abusing information technologies.

3.5 LEGAL PROVISIONS UNDER IT ACT

Hacking is a crime under sections 66 and 70 of the Indian Information Technology Act, 2000, and is punishable with imprisonment for up to three years, a fine of up to two lakh rupees, or both. However, if the hacking is performed on a secure device, the penalty is more serious.

It is necessary to note that under Indian law, a hacker who gains unauthorized access to another's computer will not be punished.It is only punishable if an intruder enters and then "destroys, deletes, or modifies any knowledge residing in a computer property, or diminishes its worth or usefulness, or harms it in any way." Unauthorized entry is only punishable if it is rendered into a "Protected system," as specified by Section 70 of the Act.

3.6 VIRUS/MALICIOUS PROGRAMMES

Viruses, worms, Trojan horses, logic bombs, hoaxes, and other malicious programmes are designed to harm the victim's computer system. They are:

a) Virus:

The virus is a malicious programme that infects an executable file and causes it to function in a different way than it was intended. It can spread by attaching itself to

executable files such as application programmes, operating systems, macros, scripts, the boot sector of a hard disk or floppy disc, and so on.

b) Worms:

Worms are malicious programmes that cause harm by multiplying and spreading copies of themselves. It does not change or delete any files, unlike viruses. It releases a worm into the internet, which slows or clogs the network because the worms keep multiplying, affecting and then sending copies to other computers.

c) Trojan Horse:

It is a seemingly innocent programme that is typically used by hackers to collect data such as passwords, credit card numbers, and other sensitive information. Such a programme can be transmitted to the victim's computer by an outsider or downloaded by the victim inadvertently from another computer, assuming it is a useful programme.

d) Logic Bomb:

It is also a malicious programme executable at a particular event. It marks the program to go into an infinite loop, crash the computer, delete data files or causes some other kind of damage to the computer or its data.

e) Hoax:

It's just a false warning about the existence of a malicious program.

Since the internet is based on the interconnection of computer networks, it is easier to send viruses or malicious programs. The most popular way for viruses and malicious programs to spread is via the internet and e-mail. Distance is no longer an issue because the whole planet has become a village.

3.7 COMPUTER SABOTAGE

The machine has grown in value as states, businesses, and individuals become increasingly reliant on computers for data storage. The days of sabotage being committed by physically damaging machines or shooting or blasting a structure are long gone. Also, insiders have the ability to inflict sabotage by using electrical short circuits or saline solution on the hardware. Computer attacks and extortion are becoming more common as people become more reliant on computer networks and

information technologies. Since vast amounts of sensitive and classified documents and records are stored on computer hard disks, hackers now have the ability to steal these data and information and then use blackmail to extort money from businesses and individuals.

3.8 COMPUTER FRAUD

The term “computer fraud” refers to common economic crimes committed by criminals using computer networks and internet access. Initially, computer frauds were restricted to data manipulation, tampering of invoices, account balances, data theft, wage payment, and so on. With the invention of the internet, computers all over the world are linked, and the potential for fraud has grown beyond national boundaries.

Certain intrinsic characteristics of the internet, such as transparency, cost-effectiveness, scope, challenges in authenticating identification, and so on, have made it difficult to detect fraudulent activity. A fake investment plan that seems legitimate and real can be advertised all over the world in seconds and at a low cost using the internet and e-mail services. As a result, it is much easier for a cyber fraudster to locate a huge number of gullible users using Internet services. The risk of such fraud is also evident in the area of e-commerce, where products and services are purchased electronically, and purchases are made using credit cards or other similar payment methods.

The Information Technology Act, 2000, made changes to the Indian Penal Code to include electronic frauds in the same category as conventional frauds. In addition, the Information Technology Act, 2000 contains provisions against fraud. For e.g., ‘tampering with computer source of text’ is punishable under Section 65 of the Act. ‘Hacking of computer system’ is punishable under Section 66 of the Act. The illegal acts of “misrepresentation” and “breach of secrecy and privacy,” respectively, are covered by sections 71 and 72 of the Act. Apart from section 100 of the Criminal Procedure Code, section 76 of the Act prescribes particular methods for the confiscation of devices used in electronic crimes, such as computers, computer systems, floppies, floppy disks, tapes, drives, and all other attachments associated dangers. Similarly, the majority of countries have enacted new legislation or amended existing legislation to make cyber fraud illegal.

3.9 COMPUTER COUNTERFEITING

Software theft is somewhat similar to computer counterfeiting. For the whole world, the validity of any document related to e-commerce is extremely important. Computer-assisted advanced printing technology is now assisting offenders in the production of counterfeit money notes, judicial and non-judicial stamps. Such paper counterfeiting is made possible by digital technologies.

Previously, provisions of the Indian Penal Code, such as Sections 417 (cheating), 465 (forgery), 471 (using as genuine a forged document known to be forged), 467 (forgery of valuable security, etc., or to gain money), etc., dealt with computer fraud and counterfeiting. However, under Section 74 of the Information Technology Act, 2000, strict rules have been made to deal with theft, forgery, and counterfeiting of digital signatures only. Section 74 of the Act deals with digital signatures only, which is one of the IT Act's major flaws.

3.9 THEFT OF TELECOMMUNICATION SERVICE AND MOBILE CLONING

Because of recent technological advances, telecommunication systems are now heavily reliant on computer networks. The repeater system, exchange, telephone networks, and other computer networks use similar technologies. As a result, it is easier for a hacker to gain access to the contact network's infrastructure and make false calls or offer free services to others.The exponential increase in the use of mobile phones has opened up a new area for illegal activity. Criminals normally break the encryption to link the handset to the service provider or use the phone for their own purposes. 'Mobile Phone Cloning' is a modern form of cybercrime that adds a new layer to the field of cybercrime. "Mobile Phone Cloning" is a crime in which "security data from one phone is re-programmed into another phone so that calls can be made from all phones but only the original is billed."

3.10 COPYRIGHT INFRINGEMENT AND SOFTWARE PIRACY

Copyrights refer to an author's or producer's exclusive right to do or authorize others to do such actions for the publishing or commercial exploitation of copyright content,

which may include a novel, literature, theatrical, musical, paintings and other creative works, cinematograph video and sound recording, and so on. Such a right is known as quid pro quo, because it is the benefit provided to the creator in exchange for his invention or intellectual property. As a result, the commercial use of copyright materials by unauthorized individuals is considered “piracy,” and is a felony against the author as well as society.

Copyright piracy is one of the most common cyber crimes perpetrated in cyberspace. Copyright preservation for publishers or creators of books, audio or video cassettes, and software programs remains one of the most difficult challenges facing law enforcement agencies all around the world. Intellectual property rights, like computer software, must be protected in order for our useful skills and lives to continue to expand. It is important for legal guardians to provide effective and sufficient protection to writers’ interests so that they can benefit from their intellectual creations.

Advanced computing technology has made it possible to pirate copyrighted works in vast quantities and at a low price. Because of widespread video theft, an original video CD of a Hindi film worth Rs. 200 is now available in the market for just Rs. 20. Since manufacturing is faster, the danger associated with physical distribution is often reduced by online distribution, piracy has been promoted and abetted on a wide scale by the internet. Apart from the tech industry, piracy has a major impact on the film and music industries. Because of the widespread proliferation of pirated copies and online downloads, the recording industry’s entire survival is in jeopardy.

For the preservation of copyright in India, the Copyright Act of 1957 was passed. The description “literary work” involves computer systems, charts, and compilations, and computer databases, according to section 2 (o) of the Act. In the case of violation of copyrights and software piracy, a legal suit can be filed to obtain an injunction, punitive damages, and benefits accounts. A criminal investigation can also be brought under the terms of Sections 63-70 of the same Act, in addition to civil proceedings.

3.11ECONOMIC ESPIONAGE

For the storage and processing of data and trade secrets, commercial and business organizations are increasingly reliant on computers. Because of this reliance on

machines, the complexity of economic espionage in cyberspace has grown. Several incidents of business secrets being stolen from reputable firms and sold to competitors have been reported all over the world. These offences have been seen involving both outsiders and employees of such businesses. Employees in private organizations are occasionally enticed by rivals to purchase trade secrets. Hacking is often done by an outsider for the purpose of collecting trade knowledge for illegal purposes.

3.12 TAX EVASION AND MONEY LAUNDERING

Money laundering is an illegal enterprise in which criminal proceeds are given the illusion of legality. To gain the requisite credibility, the criminals must first cut their hard-earned money and then spend it in another transaction. For example, a notorious criminal in Mumbai who makes money by extortion is frequently seen investing his illicit funds in Bollywood's film and music industries. Money laundering is difficult by using traditional form of cash.As a result, foreign criminals involved in drug trafficking, smuggling, and other illicit activities faced significant challenges in transporting large sums of money. In these cases, they use 'Hawala' tactics, in which a criminal sitting in Dubai can pass money to Mumbai via Hawala agents in a matter of hours. For this, an agent in Dubai accepts cash and sends a message in code words to the individual concerned in Mumbai via the internet or mobile. As such, the money is exchanged without the possibility of being intercepted or falling into the hands of law enforcement officers.

With the rise of e-commerce, tax evasion has now become much simpler. Since the volume of digital cash or e-cash in an individual's hands is not traceable in normal conditions, it has become almost impossible for a taxman or any law enforcement agency to keep track of a person engaging in e-income commerce's and spending. Following technical advancements in the cyber space, conventional anti-tax and anti-money laundering systems, as well as laws, have been unsuccessful in various countries around the world.

3.13 CYBER SQUATTING

Cyber squatting is a practice in which website names are blocked on the internet and later traced by unscrupulous individuals for commercial gain. Cyber squatting mostly

affects well-known private entities, actors, and key government institutions. To combat the illegal act, the United States of America passed the Anti-cyber Squatting Consumer Protection Act of 1999. The Act further amends Section 43 of the Trademark Act of 1946 to impose legal liability on anybody who registers, uses, or traffics in a domain name. The Act also establishes a penalty for violators and the offender is liable to pay damages and profits, as well as statutory damages ranging from $1,000 per domain, at the discretion of the judge.

3.14 INTERNET MARKETING FRAUD

Net frauds are the most recent form of cybercrime to emerge on the internet. Many fake businesses set up websites and recruit members via the internet as part of their business model. New members are paid a fee and invited to bring in more members in exchange for a commission. When the number of participants becomes unmanageable, the firms close their doors and disappear, duping all of their customers. The promised commission for adding new candidates, as well as the original payment, was forfeited by the victim members.

3.15 LET'S SUM UP

In this chapter, we have studied the classification of crimes affecting the economy along with the legal provisions pertaining to it. In furtherance, we have also seen an overview of such crimes such as hacking, cyber squatting, computer sabotage etc., and the provisions under IPC and IT Act.

3.16 FURTHER READING

- Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime. In The Economics of Information Security and Privacy. Springer Berlin Heidelberg, 265–300.
- Sam Brand and Richard Price. 2000. The economic and social costs of crime. Home Oce London
- Kshetri, Nir. (2006). The simple economics of cybercrimes. Security & Privacy, IEEE. 4. 33 - 39. 10.1109/MSP.2006.27.

- M. Riek, R. Bohme, and T. Moore. 2015. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. Dependable and Secure Computing, IEEE Transactions on PP, 99 (2015), 1–1. DOI:http://dx.doi.org/10.1109/TDSC. 2015.2410795

3.17 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is computer hacking?**

The word “computer hacking” refers to the act of manipulating, vandalism, or spying in order to gain access to a computer device.

2. **What is computer fraud?**

The term “computer fraud” refers to common economic crimes committed by criminals using computer networks and internet access.

3. **What is Trojan Horse?**

It is a seemingly innocent program that is typically used by hackers to collect data such as passwords, credit card numbers, and other sensitive information. Such a program can be transmitted to the victim’s computer by an outsider or downloaded by the victim inadvertently from another computer, assuming it is a useful program.

3.18 ACTIVITY

Elucidate the different kinds of crimes affecting economy along with the legal provisions pertaining to it. (2000-2500 words)

Unit 4: CLASSIFICATION OF CRIMES AGAINST SOCIETY AT LARGE

4

Unit Structure

4.1 Learning Objectives

4.2 Crimes affecting Nations

4.3 Crimes affecting society

4.4 Certain Shortcomings

4.5 Future Prospects and Needs

4.6 Let's sum up

4.7 Further reading

4.8 Check your progress: Possible answers

4.9 Activity

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of the cybercrimes affecting nations and society at large
- Shortcomings of provisions and definitions under IT Act, 2000
- Future prospects and needs

4.2 CRIMES AFFECTING NATIONS

a) Cyber Terrorism

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. It is a combination of cyberspace and terrorism. There isn't an appropriate definition for Cyber Terrorism which can be accepted worldwide. However, a universally acknowledged definition of Cyber Terrorism is 'A criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda'.

Cyber terrorism is the use of technology and the internet to create and spread terrorism. It is a more modern type of terrorism, and an illegal act carried out to threaten or coerce a country or its citizens into pursuing political or social objectives. To be classified as cyber terrorism, an attack must threaten or inflict violence against individuals, goods, or the government, and/or cause fear of harm among those who are affected.

The use of computer and internet networks for terrorist purposes has raised the challenge of cyber crime to the national and international community's defence. Government departments use computers to provide and communicate useful data in the transportation, medical, defence, finance, and financial services industries. Such sensitive material is not impenetrable to outsiders. They are vulnerable to attacks by hackers and terrorists, and the valuable information they provide, if intercepted, may have catastrophic consequences for the stability of their respective countries.The

thiefs of the world today with the aid of a keyboard to do more serious harm to an organization or a government than a gun or a missile.

Terrorists are using new information systems to devise tactics, collect money, generate propaganda, and exchange messages among themselves in order to carry out their plans.

b) Cyber Warfare

Another source of controversy is the use of computers by defence forces during a conflict. Most armies around the world are now entirely reliant on electronic networks for all types of defensive and offensive activities, and cyber warfare has become an integral part of military strategy. Cyber espionage to collect information about the enemy's army, as well as cyber attacks to immobilize the enemy by disrupting their information infrastructure, are also looming high.The protection of a server storing Army strategic information is a newer problem for defence authorities. The issue of electronic warfare security is now before the main international law authorities to be resolved effectively.

c) Unaccredited Calls

There are many illegal agencies running all over the world that make unaccredited international telephonic calls, causing damage to respective countries' exchequer. When an individual receives such calls, no telephone number appears on the caller ID panel of the handset. In India, phone companies like BSNL and MTNL are struggling miserably in their efforts to monitor such calls, which have uncovered a foreign SIM cloning industry that has enabled ISO calls between India and Saudi Arabia using cloned SIM cards.

In another incident, the CBI apprehended two engineers, Ashok and Suresh, who were involved in a net-heist and were using the internet to make international calls as if they were local calls. Five exchanges were confiscated in Chennai, and one such device was discovered in Hyderabad.The CBI team discovered advanced computer devices, as well as mobile handsets, wired wireless sets, switches, modems, and other equipment, connecting to internet broadband cables. They lifted foreign calls transmitted into India via Voice Over Internet Protocol (VOIP or Net telephony) and distributed them into the BSNL or MTNL networks using software-based exchanges.The BSNL and MTNL were robbed of an estimated Rs. 400 crore by such operators.

4.3 CRIMES AFFECTING SOCIETY

a) Racial Propaganda

The political leaders and their groups are often seen using computers and media networks to spread their political message. Terrorists and antisocial organizations aren't far behind in using electronic and internet networks to spread social and communal hatred ideology among the people.For example, Pakistani television networks are frequently seen spreading political and social propaganda among Kashmiris in order to instigate an indirect war. Terror groups and other radical organizations all over the world have begun to use the internet to distribute social and communal messaging among their target groups, thanks to the global spread of internet networks. Such acts of terrorism are much more successful than conventional terrorism approaches.

b) Pornography

Pornography and paedophilia dissemination on the digital internet is one of the most serious machine and internet network abuses. Paedophiles have been given a simple way to organize and spread derogatory and obscenity materials around the world thanks to the internet networks. The suspecting children's quick access to these paedophiles through the internet leaves them vulnerable to abuse.

As more classrooms and homes become wired to the internet, children now have convenient access to the internet.As a result of this incentive, children are more likely to have free access to inappropriate content that are readily accessible on the Internet.Such materials that include sexually suggestive photographs or explanations, plead hatred and bigotry, crime, substance addiction, and other criminal acts are more likely to mislead students.Cyber criminals now have a simple way to befriend a kid in a chat room without revealing his name, then manipulate him. As a result, the internet has become extremely hazardous to youth. However, it is not appropriate to keep children completely off the internet since the internet contains a wealth of valuable knowledge and instructional resources for children. On the internet, you can find useful stuff like online friendships, pen pals, and so on.Parental monitoring is necessary to prevent them from abusing the internet and falling into the hands of paedophiles and other poor actors who promote illegal acts.

Section 67 of the Information Technology Act, 2000 discusses about publishing of information which is obscene in electronic form. The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material lascivious or appeals to the prurient interest,
- Tendency to deprave and corrupt persons,
- Likely-audience,
- To read, see or hear the matter contained or embodied in electronic form.

It is important that while interpreting this provision, the court may exercise the interests of our contemporary society and particularly the influence of the obscene material in electronic form on it. For this purpose, even the State Governments may have to apprehend perpetrators of *'cyber obscenity'* by invoking local State legislation's accordingly. In the case of *Prakas (Dr.) vs State of Tamil Nadu,*[25] the petitioner was detained under Section 3(1) of the Tamil Nadu Prevention of Dangerous Activities of Bootleggers, Drug Offenders, Goondas, Immoral Traffic Offenders and Slum Grabbers Act. The main grounds of detention against the petitioner were that he was indulging in offences under Section 67 of the IT Act, 2000, Section 4 and 6 of the Indecent Representation of Women (Prohibition) Act, 1986 and under Section 27 of the Arms Act, 1959. The petitioner challenged his detention under Article 32 of the Indian Constitution.

The petition was dismissed, as the Supreme Court did not find much merit in the plea that the delay of two days in furnishing translated copies of documents had caused any prejudice to the detenu. It held that the contents of the letter received from members of the public *pro bono publico,* were not extraneous or irrelevant.

In furtherance, to combat cyber pornography, additionally, Section 67A was introduced under IT Act that talks about the punishment for publishing or transmitting material containing sexually explicit act etc. The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material containing sexually explicit act or conduct.

[25] Prakash (Dr.) v. State of Tamil Nadu, (2002) 7 SCC 759.

It is significant to note that publication or transmission in the electronic form includes dissemination, storage and transmission of information or data in electronic form.

In view of the ease with which obscene content can be replicated, misused and distributed over the Internet using all kinds of information technology and communication tools – it was felt by the lawmakers to move beyond *'likely audience'* test of Section 67 and to provide more stringent mechanism to combat obscenity in the electronic form.

The term *'sexually explicit act or conduct'* has been qualified by the word *'explicit'* meaning thereby that mere *'obscene act or conduct'* may not fall under this provision. For punishment under this section, *'publication or transmission of sexually explicit act or conduct'* is an essential ingredient. Hence the difference between Section 67 and 67A depends on the nature of obscene content.

	Section 67	**Section 67A**
Nature of offence	Punishment for publishing or transmitting obscenity in electronic form	Punishment for publishing or transmitting sexually explicit act or conduct
Applicability	Generic	Specific
Test of Obscenity	Likely audience test to prove obscenity	No likely-audience test. Whether content in question – is it patently or grossly explicit?
Punishment	First conviction – 3 years, and fine which may extend to five lakh rupees. Second conviction – 5 years and fine which may extend to 10 lakh rupees.	First conviction – 5 years, and fine which may extend to 10 lakh rupees. Second conviction – 7 years and fine which may extend to 10 lakh rupees

The amendment Act has incorporated the *Exception* as provided under Section 292 of IPC as proviso in the Sections 67 and 67A.

The Supreme Court in *Kamlesh Vaswani vs Union of India,*[26] has been approached to direct the respondents to block the pornography websites, platforms, links or downloading by whatever other Internet means or name in order to prevent easy access whether in private or public. The questions are twofold: (a) whether, pornography can be blocked in absolute forms? and (b) whether blocking of adult pornography is violative of freedom of speech and expression as enshrined under Article 19(1)(a) of the Indian Constitution? Interestingly, during the proceedings before the court, the respondent did block 847 websites, allegedly depicting child pornography content but had to hastily withdraw the order as majority of the listed website on examination found to carry only adult pornography content.

The issues referred to publication or transmission of obscene information in electronic form has to be also looked at from the perspective of *'extra-territorial'* jurisdiction and Internet technologies, keeping in view that *'obscenity'* is no longer a local and static phenomenon. It is now global and dynamic in nature and thus needs strict interpretation of statute.

4.4 CERTAIN SHORTCOMINGS

Despite the fact that there are certain definitions of contraventions and crimes, as well as their fines and sentences, certain questions remain unsolved. Many procedural forms and methods of crime identification and deterrence have seen less consideration from legislators. These flaws can be discussed under the headings below.

a) Power of Police to Enter and Search Limited to Higher Officers and to Public Places:

While the Act grants police officers up to the rank of Deputy Superintendent of Police (DSP) broad powers to access and search public places without a warrant and to apprehend without a warrant anybody who is legitimately accused of having committed, committing, or about to commit any crime under the Act, this authority is restricted to "public places" only.These felony offences can also be committed or are being performed on a wide scale from private residences and other private locations. Since police departments do not have enough DSP level officers to handle too many

[26] Kamlesh Vaswani v. Union of India, (2016) 7 SCC 592

investigations, the Act's requirement that only an officer of the rank of DSP can prosecute the case or conduct a search and seize is also a major restriction. Furthermore, such sweeping powers of search and seizure can result in violations of privacy and human rights.

b) Lacks Definition of Cyber Stalking and Harassment:

Hacking, damage to electronic source code, publication of pornographic material, and violation of a security device are all covered in Chapter XI of the Act, which is titled "offenses." Cyber stalking and other forms of violence, on the other hand, was completely ignored.

c) Improper definition of Hacking:

The meaning of "hacking" in section 66 (1) of the Act does not correspond to the generally accepted concept. The meaning of section 66 (1) is so broad that any conduct an individual engages in over the internet could be protected by the section's mischief. In addition, the term "wrongful loss" is not specified in the Act. Furthermore, there are no prescribed metrics for demonstrating the declining value of content.

d) Lacks of Steps for Checking Internet and Copyright Piracy:

Despite the fact that such infringements have been rampant since the invention of the internet, there seems to be an act of reasonable steps in the field of verifying the theft of copyright of music, lyrics, images, and other works in the Act. Violations of intellectual property rights and piracy in the cyberspace will result in a variety of civil penalties.

e) Lack of International Cooperation:

Since the effect and scope of cybercrime are global, any attempt made at the national level cannot be considered frivolous. Until proactive measures are taken at the international level by international collaboration, it is impossible to check terrorist activities perpetrated through the internet by aliens living and working from other countries. Achieving such constructive global partnership is also a long way off.

f) Lack of Appropriate Guidelines for Investigation:

In the world of cybercrime, conventional investigative techniques are incapable of detecting and collecting data. Since the cyber world is rapidly evolving, the legislation must be updated to keep up. Aside from amending the Indian Evidence

Act of 1872 and the Bankers Book Evidence Act of 1891, new strategies for making electronic documents admissible as evidence in a court of law are needed. The current techniques used by the police are also in the early stages of growth.

4.5 FUTURE PROSPECTS AND NEEDS

India's modest start in the world of cyberspace can be attributed to the passage of the Information Technology Act, 2000. This initiative is both timely and fitting, as India is now recognized as a global pioneer in the field of information technology. However, the scope of cyber legislation must be expanded to include an increasing number of cyber operations. The problem could be addressed by amending the Indian Penal Code to reflect the evolving nature of cybercrime. Legislative attention is also needed in the field of data security.Such legislative acts are required to protect Indian computer and internet users, as well as their right to privacy, including Indian organizations, corporations, business firms, and individuals.

The Indian Parliament has not dealt with procedural issues properly, such as inquiry and evidence evaluation. Sections 76, 78, and 80 of the Act deal with investigation, capture, search, and detention, as well as making the rules of the Criminal Procedure Code applicable to such admission, search, and arrests by responsible authorities. In this regard, certain required changes to the Indian Penal Code and the Indian Evidence Act have been introduced.However, since criminals are better trained than law enforcement officers, law enforcement agencies continue to face problems. Surveillance, search and arrest, forensic elements, proof gathering in transnational situations, and other issues include well-defined rules in today's world.

Special courts for the prosecution of cyber criminals should be created, and the judges who preside over them should be adequately and technically qualified to test facts technologically. Efforts can be made to raise public consciousness and create capacity within representatives of law enforcement departments and the criminal justice administration.In the police force, an adequate number of highly trained detective officers and forensic technicians should be hired, and a special cell should be established to efficiently deal with cyber crimes.

4.6 LET'S SUM UP

In this chapter, we have studied the cybercrimes affecting nations and society at large along with the shortcomings in the Information Technology Act, 2000. In furtherance, we have also seen the future prospects and needs or amendments needed in the Information Technology Act for the betterment of the society.

4.7 FURTHER READING

- Cybercrime and Society – By MajidYar, SAGE publication India Pvt. Ltd, NewDelhi.
- Cybercrime: Criminal Threat from Cyberspace. Goodman and Brenner, "Emerging Consensus on Criminal Conduct on Cyberspace", International Journal of Law and information technology, Vol. 10 No 2, Oxford University press 2002.
- Black , G. Patrick and Hawk, Kenneth R. (2010) Computer and Internet crimes, San Francisco, California [Online] available from <http://www.fd.org/pdf_lib/WS2010/WS2010_Computer_Crimes.pdf>
- Eric J. Sinrod and William P. Reilly (2000) cybercrimes: a practical approach to the application of federal computer crime laws; Santa Clara university school of law Journal vol16, number 2 [Online] available from < http://www.sinrodlaw. com/CyberCrime.pdf>

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the ingredients of Section 67 of the IT Act, 2000?**

The ingredients of offence under the said provision are:

- Publication or transmission in the electronic form,
- Any material lascivious or appeals to the prurient interest,
- Tendency to deprave and corrupt persons,
- Likely-audience,
- To read, see or hear the matter contained or embodied in electronic form.

2. **What is the meaning of unaccredited calls?**

When an individual receives such calls, no telephone number appears on the caller ID panel of the handset. This is generally known as unaccredited calls. In India, phone companies like BSNL and MTNL are struggling miserably in their efforts to monitor such calls, which have uncovered a foreign SIM cloning industry that has enabled ISO calls between India and Saudi Arabia using cloned SIM cards.

3. **What is Cyber Terrorism?**

Cyber Terrorism refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives.

4.9 ACTIVITY

Elaborate on the cybercrimes affecting the nation and society at large along with case laws/case studies? (1500-2000 words)

Block-2

LEGISLATIVE FRAMEWORK OF CYBERCRIMES

Unit 1: LEGAL ISSUES AND FRAMEWORK OFINTERCEPTING WiFi TRANSMISSIONS

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 WiFi Technology

1.4 Authentication and Privacy in the 802.11 Standard

1.5 Privacy

1.6 Eavesdropping on WiFi

1.7 Legal Framework

1.8 Fourth Amendment Expectation of Privacy in WLANs

1.9 Let's sum up

1.10 Further reading

1.11 Check your progress: Possible answers

1.12 Activity

1.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- WiFi Technology
- How privacy is infringed using WiFi Technology
- Eavesdropping on WiFi and Legal Framework

1.2 INTRODUCTION

WiFi stands for wireless fidelity (wireless) and refers to a set of protocols that enable computers and other devices to link to local area networks wirelessly. WiFi technology proliferation is a success story in standards growth, representing a demand worth more than $750 million per quarter globally (Infonetics Research). As a standard feature, most computer systems, especially laptops, come with WiFi-compliant hardware and software. Even the cheapest laptop sold at Wal-Mart, for example, comes with WiFi. Furthermore, the equipment used to set up your own WAN—using the same computers and Internet service—costs less than $100.

A variety of organizations have decided to make WiFi connectivity open to anybody who wants to use it. Dartmouth College has free WiFi in the campus; Panera Bread and several CompUSA shops around the country have free WiFi; and Bradley International Airport in Connecticut and Ft. Lauderdale Airport in Florida also have free WiFi. WiFi is no longer a technology used solely by the technologically sophisticated early adopters; it has clearly entered the mainstream in terms of acceptance and application.

1.3 WiFi TECHNOLOGY

WiFi is part of the IEEE (I-triple-E), or Institute of Electrical and Electronics Engineers. The IEEE is a standards-setting organization that established the 802 families of standards. These specifications define a framework—physical media and operating characteristics—that allows two or more devices to communicate in a network. The 802.3 protocol, which is the Ethernet interface, is the most well-known of all specifications. The Ethernet protocol specifies a physical networking method for use in a local area network (LAN). Ethernet is also the networking mode for the

vast majority of computer networks; nearly every computer sold now has an Ethernet jack for connecting to an Ethernet network. The vast expansion of computer networks in companies, classrooms, and government buildings is most likely due to the popularity of the 802.3 specification.

IEEE's 802.11 specificationsare seeing a similar surge in popularity and growth. The 802.11 protocol is a set of wireless local area network standards (WLANs). It specifies the form of physical communication between network devices, similar to the 802.3 standards, except instead of communication over a physical connection via cabling, the 802.11 standard specifies the communication between devices through infrared and radio frequency (RF) transmissions.While infrared has been useful in some situations—for example, short-range wireless printing—it has been overshadowed by the use of radio frequency transmissions.

Each computer on a WiFi network must have a wireless card or an 802.11 compliant radio transceiver in order to link to the network. Some computers have built-in wireless cards, while others need an extra wireless card, while still others will need to use a PCMCIA slot or a USB port to access one. A transceiver tuned to a specific frequency, as specified by the 802.11 standard, is included inside this wireless card. An access point is a system that functions as a connector between devices on the wireless network and others on the wired local area network.The access point is configured by the network user, and authentication and encryption solutions are available—most security features are disabled by default. The wireless card in a computer (or other device) communicates with the access point to transmit data and network management information over the selected radio frequency.

1.4 AUTHENTICATION AND PRIVACY IN THE 802.11 STANDARD

It's worth noting that both authentication (who is able to connect to the network) and anonymity (who is allowed to access details off the network) are discussed in the 802.11 guidelines. Users of WiFi systems, on the other hand, seldom take the time to correctly install their WiFi network. A cellular network is not the same as a physical-wired network. To link to a physical network, one must first have physical access to the network. As a consequence, physical authentication is critical for authenticating users in a physical network.Wireless networks, on the other hand, do

not remain conveniently enclosed inside the walls of a building—authentication is used to determine who is placed on a WLAN.

“The service used to determine the status of one station as a part of the collection of stations permitted to associate with another station,” according to the 802 guidelines. (R2003) ANSI/IEEE Std 802.11, 1999 Edition) As a result, there must be a way to restrict entry to a certain WLAN—and there is. One approach is to use MAC address authentication to control access. The access point maintains a list of approved MAC addresses during this process. WLAN connections would be enabled for network interface cards with MAC addresses on the accepted list. The entry point would not let you in if your name isn't on the list.

Another method for controlling authentication is encryption. WLANs can be programmed to use a range of encryption schemes, the most popular of which are WEP and WPA. By restricting the decryption of WLAN signals, encryption regulates authentication. To decode the signal, approved users must have the requisite secret key—indeed, they must have the correct credentials to bind to the access point at all.

To assist the user with authentication, one would presume the equipment would allow either MAC access control or one of the encryption schemes by design. This is not the case, though. The default configuration of most access points is known as Open Device Authentication in the 802.11 protocol. Any system that requests authentication can be authenticated and connected to the WLAN using this scheme. Excluding the fact that more reliable methods of authentication exist—MAC filtering and encryption—the 802.11 protocol describes open framework authentication as the default setting for 802.11 applications.

1.5 PRIVACY

The routing of information protects secrecy in a wired LAN. On a LAN, routers and switches monitor the flow of data such that computers on the LAN receive either data that is directly addressed to them or data that is broadcast to all devices. Eavesdropping on a wired network, on the other hand, can be impossible, requiring physical access to the network and/or direct access to the computer of interest. If anyone wanted to listen in on data traffic on the cable between computer X and the network switch, for example, the eavesdropper would only be able to see traffic transmitted to computer X.

Inside a WLAN, data is transmitted over RF transmissions to all computers connected to the WLAN; data is not limited to moving in specific cables to a single computer. Since RF cannot be contained, data intended for any of the devices in a WLAN can be viewed at a much higher level without having physical access to the network. Furthermore, the radio waves produced by the access points often surpass the confines of the space or building in which they are located and intended for use.

1.6 EAVESDROPPING ON WiFi

Eavesdropping on WiFi communications does not take a lot of experience or ability, and the equipment, both hardware and software, is readily accessible. There are a range of tech products that can both locate and listen in on WiFi transmissions. For the most part, these software packages are fully legal network analyzers that network operators use to debug networks and detect unwanted access points.
Any non-encrypted contact over the WAN can be snatched from the airwaves and shown. Limiting who connects to a network makes the entire network secure, specifically the details on other computers on the network, but it does little to deter people from intercepting unencrypted transmissions. Transmissions must be encrypted to prevent the contents of the transmission from being accessed by any 802.11-equipped computer.

1.7 LEGAL FRAMEWORK

We must examine how current regulations apply to WiFi technologies in order to fully comprehend the legitimacy of WiFi eavesdropping. As we'll see, federal laws governing the interception of different forms of electronic messages don't seem to extend to WiFi transmissions.

- ***The Electronic Communications Privacy Act (ECPA)***

Despite the fact thatWiFi messages come within the definition of electronic communications as established by the ECPA, the signals sent by WiFi devices are open to the general public unless they are secured. As a consequence, the interception of non-encrypted WiFi signals that are not transmitted by a common carrier is not protected by ECPA.

Under the ECPA, WiFi messages will be called “electronic communications.” The Electronic Communications Privacy Act (ECPA) forbids the interception of all electronic communications, regardless of the physical medium of transmission (USC 18 §2510). “Any transmission of signs, messages, writing, pictures, sounds, data, or intelligence of any kind conveyed in whole or in part by a cable, antenna, electromagnetic, photoelectronic, or photo-optical device that affects interstate or international commerce,” according to the ECPA.In the past, judges have used a vague description of what constitutes interstate commerce.As a consequence, using WLANs to transfer data, particularly when connecting to the Internet, would be called “electronic communications” under the ECPA.

A data trespasser is someone who gains unauthorized access to a protected computer and therefore has no fair sense of privacy in any contact sent to, from, or from the protected computer (USC 18 § 2510). It’s worth noting that, like the CFAA, this concept makes no allowances for wireless eavesdroppers who don’t need entry. The ECPA (USC 18 §2511 (1)(a)) punishes someone who “intentionally intercepts, endeavours to intercept, or procures some other entity to intercept or endeavour to intercept any cable, oral, or electronic contact.”

Despite the fact thatWiFi transmissions fall under the ECPA’s concept of electronic communications, the statute exempts electronic communications that are easily accessible to the general public.Typical WiFi broadcasts have a lot of characteristics that make them easily available to the general public.As a result, it seems that the ECPA does not apply to most WiFi transmissions.

WiFi transmissions are not scrambled or encrypted, for instance. The 802.11 standard’s default configuration is open device authentication with no encryption.As a result, 802.11 WiFi networks do not follow these requirements in their default configuration, with no encryption allowed. Next, WiFi broadcasts do not use modulation techniques whose basic parameters have been kept hidden from the public in order to protect the secrecy of such correspondence. The IEEE 802.11 protocol is open to the public. Furthermore, the requisite hardware and software are not limited or regulated objects, and the hardware is often used as a regular feature in many computers.

Only WiFi messages transmitted over a single carrier’s contact channel are covered by the ECPA. A national carrier is a company that charges the general public for communication services. The ECPA would apply to a number of well-known carriers

that operate WiFi networks. The ECPA, on the other hand, does not apply if the WiFi network in question is operated by a private citizen or other entity that is not in the business of providing internet services. See *Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998)* (defendant did not provide electronic communication service to the public and therefore could not be sued under the ECPA).

- ***Telecommunications Act***

Since WiFi messages may be accessed by the general public, the Telecommunications Act would not seem to regulate WiFi interceptions. “No person not allowed by the sender shall intercept any radio communication and divulge or publish the presence, contents, substance, purport, consequence, or sense of such intercepted communication to another person,” according to the Telecommunications Act. This clause would not refer to accessing, disclosing, printing, or using the contents of any radio correspondence broadcast by any station for the general public...” 605 of the United States Code (emphasis added).

- ***Computer Fraud and Abuse Act***

Since the Computer Fraud and Abuse Act (CFAA) is mainly based on manipulating (Kern, 2004) computer networks, it does not tend to extend to the intercept of WiFi signals. While there does not seem to be any direct case law on the subject, passively monitoring a WiFi contact would not appear to include manipulating the person’s device in the sense that the word is commonly known. The first six major legislative breaches deal with gaining improper access to a computer device, while the seventh deals with rendering threats of harm to a safe system (the following things have been paraphrased for clarity):

a) Unauthorized access to a device containing classified government records.
b) Obtaining financial information from a financial institution or card issuer, any US government papers, or information from a secure computer relating to domestic or international trade without permission or beyond permitted access.
c) Deliberately and without permission accesses any nonpublic device of a United States department or organization.
d) Accesses a secure device without permission or exceeds permitted access in order to conduct or further a crime with the intent to defraud.

e) Gains access to a secure device and deliberately disseminates malicious code or causes injury, whether purposely or accidentally, or tries to obtain access that will result in a loss of $5000 or more, bodily injury, medical care alteration, a threat to public safety, or disruption to a government structure.
f) Traffics in any password or related information from which a device can be accessed without permission, knowing and with intent to defraud, if— (A) such trafficking involves interstate or international commerce; or (B) such computer is used by or by the United States Government.
g) Any person who transmits any message involving any attempt to inflict harm to a protected device with the intent to extort money or other valuables.

Eavesdropping on WiFi may be achieved passively, with the eavesdropping device emitting no outgoing info. To collect data carried on radio frequency transmissions, no link to an access point is necessary.

1.8 FOURTH AMENDMENT EXPECTATION OF PRIVACY IN WLANs

Despite the fact that Congress has opted not to pass laws banning the surveillance of WiFi traffic, cyber fraud agents are also prohibited from performing unlawful searches under the Fourth Amendment as law enforcement officers. Only those areas in which the target of the search has shown an actual (subjective) presumption of privacy and the expectation is one that society is willing to consider as “fair” are protected by the constitution (Katz v. United States, 389 U.S. 347, 361 (1967)). Although an individual has a constitutionally-protected expectation of privacy in his home,“[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection” (Katz, 389 U.S. at 351).“The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares” (California v. Ciraolo, 476 U.S. 207, 213 (1986)). “Nor does the mere fact that an individual has taken measures to restrict some views of his activities to preclude an officer’s observations from a public vantage point where he has a right to be and which renders the activities clearly visible” Id. (citing United States v. Knotts, 460 U.S. 276, 282 (1983)).

The argument then becomes whether a fair presumption of privacy in electronic messages exchanged through WiFi exists under the Fourth Amendment. While the case is yet to be resolved, the best opinion seems to be that such a privacy expectation would not be fair under the Fourth Amendment.It is a fundamental feature of WiFi communications that, at the user's discretion, may be encrypted and thereby easily hidden from public view. As a consequence, if a person decides not to use the built-in encryption—which is expressly defined in the WiFi standard—courts are likely to infer that the WiFi user has given up any fair assurance of privacy(see United States v. Granderson, 182 F. Supp. 2d 315, 321–22 (2001) defendant had no reasonable expectation of privacy when conducting drug activities behind a boarded-up window that had a slot between the boards since the defendant easily could have shielded his activities from public view by taking simple and obvious steps).

1.9 LET'S SUM UP

In this chapter, we have studied the meaning and how WiFi technology works along with understanding as to how privacy is infringed due to the usage of this technology with the help of the US laws. Furthermore, we also studied on eavesdropping on WiFi and legislative framework of the same along with the fourth amendment expectation of privacy in WLANs.

1.10 FURTHER READING

- Kern, Benjamin D. 2004. Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. Santa Clara Computer and High Technology Law Journal.
- Jain, B. 8,736 phone and e-mail accounts tapped by different government agencies in July. September 17th 2011. Available at: http://articles.economictimes.indiatimes.com/2011-09-17/news/30169231_1_phone-tap-e-mail-accounts-indian-telegraph-act
- Chaudhary, A. BlackBerry's Tussle with Indian Govt. Finally Ends; BB Provides Interception System. http://www.medianama.com/2013/07/223-

blackberrys-tussle-with-indian-govt-finally-ends-bb-provides-interception-system/

- Report of the Group of Experts on Privacy. Available at: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of WiFi?**

WiFi stands for wireless fidelity (wireless) and refers to a set of protocols that enable computers and other devices to link to local area networks wirelessly.

2. **What is the meaning of authentication?**

Authentication is defined in the 802 standards as “The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.”

3. **How are WLANs set up?**

WLANs can be programmed to use a range of encryption schemes, the most popular of which are WEP and WPA. By restricting the decryption of WLAN signals, encryption regulates authentication. To decode the signal, approved users must have the requisite secret key—indeed, they must have the correct credentials to bind to the access point at all.

4. **What does 802.11 standard state?**

The 802.11 standard clearly articulates that additional privacy measures, primarily authentication measures such as MAC filtering and encryption, are needed to prohibit any other 802.11 equipped device from connecting to the wireless access point

1.12 ACTIVITY

Elucidate how WiFi signals are interrupted, along with a few case studies. (1500-2000 words)

Unit 2: CYBER SECURITY AND INTERNATIONAL LEGAL ASPECTS

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 What is Cybersecurity in U.S.?

2.4 Current U.S. Comprehensive National Cybersecurity Strategy

2.5 International Comprehensive Cybersecurity Strategy

2.6 Let's sum up

2.7 Further reading

2.8 Check your progress: Possible answers

2.9 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Cybersecurity in U.S.
- U.S. Comprehensive National Cybersecurity strategy
- International comprehensive cybersecurity strategy

2.2 INTRODUCTION

Cyberspace, like a virtual battleground, has become a battleground for the appropriation of personal data, espionage of scientific, economic, and commercial assets of companies that fall prey to competitors or foreign powers, disruption of services essential to the economy and daily life, compromise of information related to our sovereignty, and even assassination.

This “virtual battleground” in cyberspace has only increased global security visibility and has had a significant effect on global political stability, cutting a vast swath across physical territorial borders and affecting the security of people, private companies, societies, and global nation-state governance and stability.The Internet is integral to many international trade and enterprise growth activities in both developed and developing countries. For example, digital technology underpins Canada’s entire economy, with 87 percent of commercial businesses dependent on the Internet to do business in 2012.

Individuals can use the Internet to mobilize and inform others about current political activities or events affecting others in a specific community and can operate individual water systems. The Internet offers a nearly anonymous avenue for world people whose freedom of expression is limited or forbidden, where individuals can communicate without government interference and intrusion, use the Internet to rally and warn others about current political developments or events involving others in a particular society, and run individual water systems. People and factions with sinister agendas that wish to destabilize or overthrow governments or perform acts of terrorism, on the other hand, can gain access to and use the same rights.

2.3 WHAT IS CYBERSECURITY IN U.S.?

The legal playing field on which local, state, and federal institutions in the United States, foreign organizations, and European Union (EU) member states target their

legal bat to oversee, rule, and defend their defined tangible and intangible properties from cybercrime, espionage, and assault brings common terminology into play, which at first glance seems to be equivalent because the players wear the same uniforms.However, upon closer examination, some players have merely adopted a term without ever assigning a particular meaning to that term, while others have adopted a specific definition that does not correspond to any scientific or actual statistical context. In all events the willingness of all players to recognise their strengths and disadvantages, to produce sound gaming statistics and to create an easy-to-understand rules book which is technically reasonable and smooth to use, will not be able to develop and provide standardized concepts compatible with overall strategy, legal framework and theoretical grounds.

The development and adoption of specific meanings for the primary terms of art dealing with the protection of various informational structures and their physical and virtual devices, all of which are interconnected through the Internet, has been defined as a necessary component if and when cybersecurity is established as a discipline. The experimental method, which involves the repeatability of experiments based on precise meanings and conditions, will be extended to the study of cybersecurity as a result of this development.“It’s essential to provide specific meanings. It would not be necessary to raise the degree of rigour until a precise collection of items can be studied carefully and clearly.”

Recognizing that standardized and globally accepted definitions for significant and repeating terms of art affecting cybersecurity do not yet exist among global nation-states, businesses, and individual stakeholders, an examination of the relevant U.S. and international legal environments must identify, at the very least, what has been identified as a definition, or the lack thereof, for the aforementioned terms of art.What exactly does the term “cybersecurity” imply, and is that meaning broad enough to be applicable across borders? Is that term widely agreed across the globe, or is it finite, exclusive, and exclusive to only a few nation-states? The expression “cybersecurity” tends to be used interchangeably, just as the term “glue.”As we all know, not all glues are made equal, which means that the additives used in particular forms of glue will decide whether the glue sticks or not, or, even worse, will muck it up and produce more complications than remedies. Definitions can be compared in the same way.Because of the breadth and reach of coverage, a concept of cybersecurity

must properly consider and resolve the physical and virtual existence of the objects be protected.

Cybersecurity is a multifaceted challenge, and regulatory and legislative analyses of cybersecurity problems must differentiate not only between various cyber threat entities, such as nation-states, terrorist groups, terrorists, and malicious hackers but also between different forms of cyber threats. Threats to vital facilities, which could result in a loss of life or substantial economic damage, and threats to intellectual property, which could affect our nation's long-term prosperity, are examples of cyber threats.

2.4 CURRENT U.S. COMPREHENSIVE NATIONAL CYBERSECURITY STRATEGY

In general, new federal and state cybersecurity policies have evolved in response to abuses and malicious activities in particular economic markets, either directly or indirectly.Despite the fact that a slew of bills has recently been introduced to establish a standardized umbrella federal cybersecurity legal structure that will protect all government and private computer and network networks, none of them has been effectively implemented into legislation.In February 2003, the White House released The National Strategy to Protect Cyberspace, which was the first national cybersecurity policy released by the White House under then-President George W. Bush. Bush defined, suggested, and stressed the role of a public–private relationship in implementing the national strategy to protect cyberspace, as well as the importance of private sector engagement.Bush's cyberspace policy prioritized five issues: (1) establishing a strategic cyberspace security council, (2) a cyberspace threat and risk prevention initiative, (3) a cyberspace security awareness program, (4) a roadmap to protect federal cyberspace, and (5) national and international cyberspace collaboration.

The Comprehensive National Cybersecurity Initiative (CNCI) began as a classified offshoot of Bush's National Strategy, despite the fact that these five policy goals would not result in the passage of any substantive legislation.The Center for Strategic and International Studies (CSIS) named a Commission on Cybersecurity for the 44th Presidency ("Commission") in December 2008, which released a report with three main findings: "(1) Cybersecurity is already a significant national security

issue for the United States; (2) decisions and activities must protect privacy and civil liberties; and (3) only a holistic national security policy that encompasses all domestic and foreign facets of cybersecurity can make us safer."

President Barack Obama released a revamped and modified CNCI as National Security Presidential Directive 54 on March 2, 2010, in response to the CSIS Commission's findings, which specifically discussed cybersecurity of federal networks, both classified and civilian; required the use of EINSTEIN 2, an intrusion prevention system, across all federal systems; and decreased government spending.In the absence of a legally binding cybersecurity standard, the Obama White House released Executive Order (EO) 13636, Strengthening Critical Infrastructure Protection, on February 12, 2013, which defines a national policy on cyber intrusions, describes the essence and extent of the United States' national policy on critical infrastructure security, and establishes a mechanism for information sharingand coordination with private entities to enhance and better protect critical infrastructure assets, defines critical infrastructures and critical infrastructure sectors, and directs the development of standards and a framework for improved cybersecurity of critical infrastructures.The EO also orders the Secretary of the Department of Homeland Security to protect citizens' privacy and civil rights and to ensure their participation in the operation and enforcement of the Order's mandates by implementing the Fair Information Practice Guidelines and other related "privacy and civil rights policies, standards, and mechanisms."

2.5 INTERNATIONAL COMPREHENSIVE CYBERSECURITY STRATEGY

Although a number of international organizations are forming alliances among member countries around the world, the United Nations (UN) and the North Atlantic Treaty Organization (NATO) are two international bodies whose activities are raising global concern about cybersecurity, increased growth, and access to Internet connectivity (NATO). NATO's activities in support of its politico-military mission to provide diplomatic and unified security for its European members are coordinated and supplemented by the UN.

a) UN Cybersecurity Policy and Strategy

The United Nations (UN) is an international organization established on October 24, 1945, with the goals of maintaining peace, establishing “good ties among nations,” assisting “nations in working together to improve the lives of poor people,” and coordinating nations’ efforts to “achieve these goals.” There are officially 193 countries that are part of the United Nations.The UN, as an international body, effectively functions as a “standard entrepreneur” and agent of change to its member nations and the world at large, offering analysis and proposed models on a range of topics, including cybersecurity and international Internet regulation, since it has no jurisdiction over its member nations to implement its global mandate.The UN Charter specifies six main institutions to act and self-govern: the General Assembly, Security Council, Economic and Social Council, Trusteeship Council, International Court of Justice, and a Secretariat (Chapter 3, Article 7). Chapter 4, Article 22 allows the principal organs to join additional committees or subsidiaries to assist them in carrying out their responsibilities as appropriate. 60 Chapter 9, Article 57,61 establishes the use of specialist organizations controlled by interagency agreements issued by the Economic and Social Council in accordance with Chapter 10, Article 63.

The Internet Governance Forum (IGF) and the International Telecommunication Union (ITU) are two of the most relevant international multi-stakeholder advisory bodies working under the United Nations umbrella, tasked with investigating, collaborating, and consulting on global issues affecting Internet governance and cybersecurity.Although neither the IGF nor the ITU has the power to enact or implement legislation, they both serve as “think tanks” that collaborate and gather information, feedback, and analysis from a range of outlets, including scholars, private enterprise, government agencies, the general public, advocacy organizations, and others, in order to propose best industry practices for remaining cyber secure and keeping the internet safe.

The IGF is an online multi-stakeholder forum where public and private people and organizations from around the world can gather to discuss topics and concerns that affect Internet governance. The IGF was founded in 2006 by the UN Secretary-General, who is also the head of the UN Secretariat, “to assist the UN Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new multi-stakeholder policy discussion forum.”In relation to the IGF, the ITU is an UN-affiliated organization with “191

Member States and more than 700 Sector Members and Associates." In its position as the UN's leader for information and communication technology, the ITU represents three main sectors: Standardization, growth, and radio communication.Cyber attacks against member constituencies and processes are one of the most serious issues facing the world today, according to a consensus of UN members. Since the Russian government first submitted a cybercrime resolution to the General Assembly in 1998, and an explosive growth boom on the Internet started in 1998, 77 Maurer pins raised UN interest and escalation of cyber challenges to the forefront.

b) NATO Cybersecurity Policy and Strategy

Following continuing Soviet threats to the stability of newly formed nations seeking to rebound from the destruction of World War II, the North American Treaty ("Treaty") was signed on April 4, 1949, resulting in the establishment of NATO. NATO now consists of 28 European and North American countries.NATO has provided politico-military assistance, training, education, and peacekeeping to member nations who have been targeted or are engaged in external conflict since its establishment. Although NATO prioritizes peace in settling future disputes among nations, the Treaty imposes a clear measure of alliance unity by tying adverse action on all members in the event of an attack on one of them. Article 5 of the North American Treaty reflects this critical pillar:

The Parties agree that if an Armed Attack is carried out against one or more of them in Europe or North America, the Parties shall assist the Parties, if an Armed Attack takes place in any case, in exercising their right to individual and collective self-defense, recognized in Article 51 of the Charter of the United Nations, and that the Party or Parties attacked therefrom shall assist.

Cyber threats, which NATO tackles independently via its members' networks, an articulated cybersecurity strategy81, and the NATO Cooperative Cyber DefenseCenter of Excellence in Tallinn, Estonia, can be prompted by this unity in security to NATO members.On December 27, 2013, the United Nations explicitly stated that behaviour in cyberspace is governed by international law83, bolstering the effect and current applicability of NATO's Article 5 in the event of nation-sponsored or launched cyberattacks against NATO members.

c) EU Data Protection

The European Union (EU) is an economic and political international organization made up of 28 European member states whose members govern collectively by a series of interconnected structures, the most important of which are the Euro Parliament, the Council of European Union (EU Council), and the European Commission (EU Commission).The Euro Parliament, according to its website, is made up of representatives who are directly elected by EU citizens every five years.
Along with the Council of the European Union ("the Council"), Parliament is one of the EU's key law-making organs. The European Parliament holds three core functions:

- Debating and passing European laws, with the Council.
- Scrutinizing other EU institutions, particularly the Commission, to make sure they are working democratically.
- Debating and adopting the EU's budget, with the Council.

The European Union Council is a governing body made up of national ministers from each EU member country who meet to "adopt laws and coordinate policies." The EU Council is responsible for authorizing the annual budget, implementing EU legislation, organizing member countries' economic strategies, enforcing negotiations between the EU and other nations, establishing EU international and security policies, and promoting coordination between prosecutorial and law enforcement agencies.
The legislative authority that the EU's governing bodies exercise is founded on two main treaties that grant them the authority and power to issue legislation, orders, resolutions, advice, and opinions. A released directive, as opposed to a law, is "a statutory act that lays out an aim that all EU countries must meet."Specific nations, on the other hand, must determine how to proceed."On October 24, 1995, the Euro Parliament and EU Council released Directive 95/46/EC (the "Information Security Directive") on the protection of personal data of individuals and the free flow of such data within the EU, according to former Article 7(a) of the Treaty of European Union.
In recent years, the EU Court of Justice has interpreted the language of Article 7(f) of the Data Protection Directive with that of Article 8 of the EU Charter to provide a distinct and powerful individual right to data protection that precludes laws of member states that seek to release personal data without the consent of the data subject.The EU Commission released its proposal on the issuance of regulation on

January 25, 2012, in response to the dynamic nature of the Internet and the constantly changing technological development impacting the collection, use, and distribution of electronic data, as well as the potential erosion of the Data Protection Directive's ability to protect personal data.The draft law has five key components: (1) geographical reach, which guarantees a constitutional right to data security regardless of the geophysical position of the enterprise or its servers; (2) international transactions allowed where data protection is guaranteed; (3) compliance, which requires substantial penalties for foreign companies who do not comply with EU data protection rights; and (4) development of substantive guidelines for the security of personal data exchanged with law enforcement by cloud storage data processors, providing specific rules on responsibilities and liabilities.

Despite the lack of an EU law, the European Court of Justice recently approved the principle of the "freedom to be lost" based on existing Data Security Directive provisions. The European Court of Justice ordered Google, Inc. and its foreign branches ("Google") conducting business with the EU to respect individual EU citizen requests to remove personal data from Google search engines on May 13, 2014.

2.6 LET'S SUM UP

In this chapter, we have studied how cybersecurity has been defined in U.S. along with the comprehensive National Cybersecurity Strategy and its historicial development. Further, we also have studied the U.N. cybersecurity policy and strategy along with NATO and U.S. policy and strategy.

2.7 FURTHER READING

- European Parliament, Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy, Industry, Research and Energy. September 2013. "Data and Security Breaches and Cyber-Security Strategies in the E.U. and Its International Counterparts." IP/A/ITRE/NT/2013-5, PE 507.476, 41. Available at http://www.europarl.euro.eu
- NATO Cooperative Cyber Defence Center of Excellence. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare, 45. Available at http://issuu .com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381#

- For further information concerning the ITU and its recommendations, see http://www.itu.int, International Telecommunications Union. April 2008. “Series X: Data Networks, Open Systems Communications and Security,” 2.

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the meaning of cybersecurity?**

Cybersecurity is a multifaceted challenge, and regulatory and legislative analyses of cybersecurity problems must differentiate not only between various cyber threat entities, such as nation-states, terrorist groups, terrorists, and malicious hackers but also between different forms of cyber threats.

2. **What are IGF and ITU?**

The Internet Governance Forum (IGF) and the International Telecommunication Union (ITU) are two of the most relevant international multi-stakeholder advisory bodies working under the United Nations umbrella, tasked with investigating, collaborating, and consulting on global issues affecting Internet governance and cybersecurity.

3. **What are the three core functions of European Parliament?**

The European Parliament holds three core functions:

- Debating and passing European laws, with the Council.
- Scrutinizing other EU institutions, particularly the Commission, to make sure they are working democratically.
- Debating and adopting the EU’s budget, with the Council.

2.9 ACTIVITY

Elucidate NATO, U.N. and U.S. Cybersecurity policies and strategies in detail (2500-3000 words).

Unit 3: MAPPING THE COSTS OF CYBER CRIME

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Economic concepts

3.4 Cost of Cybercrime framework

3.5 Understanding scale, trends and measurement of cyber dependent crimes.

3.6 Three steps to unlock cybersecurity value

3.7 Let's sum up

3.8 Further reading

3.9 Check your progress: Possible Answers

3.10 Activity

3.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- Cost of cybercrime through research data presented by UK agencies.
- How to handle the cybercrime situation.

3.2 INTRODUCTION

The word "cybercrime" is not a legal term. As a result, it holds some contextual mutability, such as ‘cyberspace' criminality (Gibson 1982, 1984) and ‘the transformation of illicit or dangerous behavior by networked infrastructure' (Gibson 1982, 1984). (Wall 2007: 10). As a result, cybercrime may refer to the use of computers to aid in the commission of "traditional" crimes, either within specific structures or through global networks. It may also involve cybercrimes that are entirely mediated by technology, referred to as "third generation" cybercrimes (Wall 2007: 10). Such cybercrimes, such as spam e-mail, are purely a product of the Internet and would not occur otherwise. Many of the so-called cybercrimes that have sparked outrage over the last decade, though, are not actually offences in the legal sense. In essence, the suffix of "crime" is applied to actions that do not easily fall into the scope of criminal law. As a consequence, there isn't necessarily a legal justification for such "cybercrimes." They are more contentious harms that fall outside of the criminal justice system's control and practice, such as cyber-rape (MacKinnon 1997) and virtual reality vandalism (Williams 2006).

Despite the fact that ‘What is the essence and scale of cybercrime?' seems to be a straightforward query, it is actually difficult to respond in terms of frequency and distribution throughout societies. Crime prevention programs, on the other hand, are typically based on statistics that can accurately represent both the kinds of offenses that are being committed and the frequency at which they are occurring. Similarly, the degree to which crime rates have reduced, or not, is a clear indicator of the success of criminal justice responses.A collection of consistent, accurate data will help advise and assess policy responses to cybercrime. Attempting to map and quantify cybercrime is appealing for this primary purpose. While the security group is "prone to leap to management while bypassing calculation," as Wade Baker put it, "measurement allows management."

Estimates of crime costs will aid the government in achieving the best effect on crime with the least amount of money spent. The statistics will be used to measure and monitor measures aimed at minimizing crime. They will assist the government in prioritizing measures that have the largest effect on crime-related damage, rather than just the amount of crimes (Home Office, 2000, p 7).The Home Office has previously published research examining the costs of traditional crimes such as burglary and violent crimes. Previously, the Home Office conducted reports on the costs of traditional offences like robbery and violent crimes. A research by the Home Office (2013b) measured the social and economic consequences of organized crime. Cyber terrorism, on the other hand, has not been included in all such figures to date due to the difficulties in accurately estimating costs. In light of the emerging challenges posed by cyber-enabled and cyber-dependent offences, it is now necessary to examine the effects of new digital crime forms and aim to measure the costs they have on the UK economy.The study on the effects of crime has taken an iterative approach, with revisions released as approaches and expense forecasts have changed. This has enabled cost of crime analysis to guide progress in future research while also providing an easy-to-access summary of the most well-known cost figures for the research community. In order to form an overall view of the cost of crime, the costs of crime study has concentrated on the economic cost to the UK per incident, and has separately used figures of the prevalence of crime.The costs considered in this study were divided into three categories: costs in preparation, costs as a result, and costs in reaction.

3.3 ECONOMIC CONCEPTS

The Costs of Cyber Crime Working Group funded a study to create a costs of cyber crime system to outline and help explain the multiple assessments of cyber crime costs based on the lessons learnt from the literature review exercise and a commitment to encourage accuracy in future study. Dr. Adam Bossler, in collaboration with Home Office Analysis and Insight, worked on this initiative.The system strategy was built on previous Home Office studies into the effects of crime, and the costs were broken down into the same three categories:

- costs in preparation

- costs as a resultand
- costs in reaction.

This section introduces the economic principles that underpin the system, followed by a summary of the framework itself. The report's subsequent chapters address how researchers should use the methodology to ensure that prospective research projects are complementary and clear in approach. The definition of economic cost was used in this project to illustrate the full effect of cyber fraud on the UK economy. HM Treasury's Green Book advice from 2003 was used to develop economic principles.The idea of opportunity cost is a central economic concept used in the system for calculating the effects of cybercrime. This applies to "the worth of the most valuable of alternate purposes," which simply means the value of assets or services if they were put to other uses rather than being attributed to cybercrime in this situation. The definition of opportunity cost helps researchers to value the capital, such as people or money, that would be freed up if cyber crime did not occur in the United Kingdom. It is therefore necessary to understand the principle of transfer payments and their position within the system. If there is no product or service in exchange, transfer payments exist in an economy. Subsidies and casinos are examples of such transactions. Transfer fees are not used in the costs of crime context because they are not considered a societal expense and are merely financial transfers within the UK economy. Fines handed out to enterprises for not adequately protecting data from cybercriminals are an example of transfer fees related to the costs of cyber crime; this is not seen as a cost to the economy, but rather as a financial burden to businesses.

Furthermore, under recommendations from the Home Office's costs of crime work, reimbursement premiums to victims of cybercrime are not included in the costs of cybercrime scheme. Insurance lawsuits were left out so the sharing of funds between insurers and insurance providers, as well as payments from insurance companies to victims, was not considered a societal cost. Insurance claims, on the other hand, are not included in the cyber crime framework's charges, but insurance management expenses are.They are the costs of insurance providers' personnel, facilities, and supplies, and they pose an opportunity loss to society because these services would be opened up and used elsewhere in the economy if cyber terrorism

did not exist.

3.4 COSTS OF CYBER CRIME FRAMEWORK

Costs have been divided into three groups that reflect the different levels of how victims experience the costs of cyber crime:

- costs in advance of cyber crime,
- costs as a result of cyber crime, and
- costs in reaction to cyber crime, as previously mentioned.

Individuals and companies typically use costs in advance as a protective mechanism to deter violence. Expenditure on anti-virus applications is one example. As a consequence, costs look at costs that arise as a direct result of a felony, which usually take the form of collateral damage or income wasted. It does, however, contain the mental and physical costs of violence. Individuals had little to little power over these expenses. Costs in action examine the costs incurred as a result of a decision about how to respond to a given crime.

This usually entails reactions from law enforcement and the criminal justice system, all of which are burdened and lose money as a result of cybercrime. There are costs over which you usually have more leverage over what you can do. The costs of cyber crime system is an effort to consolidate all that is known about the costs into a single table, allowing for a clearer view of existing research discrepancies (as of 2016) and promoting further research.The goal was to make it easier for researchers to figure out what the many different component costs of cyber crime are, and how they converge to shape the total cost of cyber crime – a resource that didn't exist in the literature before.

Considering costs in this manner can aid researchers in identifying research gaps and encouraging the creation of coherent research that can be used together in the future to better appreciate the potential cost of cyber crime.

THE COSTS OF CYBER CRIME FRAMEWORK – SUMMARY OF COST TYPES

Technology costs

• Computer security protection software/products (for example, anti-virus, patching)

- Introduction of new/additional technologies Training
- Cybersecurity training/education
- Training for law enforcement investigators and officers
- Training of court and legal personnel

Security practices/behaviours

- Implementing cybersecurity practices
- Usability/user impact as a result of increased security procedures
- Switching internet service providers (ISPs), security providers or products to increase security
- Vetting staff or contractors for security purposes
- Monitoring third parties' security
- Checking credit histories/scores
- Avoidance of the internet and/or other technologies (amongst non-users)

Government activities

- Drafting and creating new legislation
- Efforts to educate public on new legislation
- Implementation of national awareness raising/protection campaigns

Other

- Cyber-insurance administration
- Consumer credit/identity protection services (for example, CIFAS, a fraud protection organisation)
- Fear/worry about cyber crime
- Collection and compilation of cyber crime statistics

3.5 UNDERSTANDING SCALE, TRENDS AND MEASUREMENT OF CYBER DEPENDENT CRIMES

The aim of this study, conducted by David Emm, Professor Steve Furnell and Dr Maria Papadaki, was to provide a better understanding of the range of measures used to assess the prevalence or incidence of cyber-dependent crimes, including:

- viruses and other malware;
- denial of service or distributed denial of service (DDoS); and
- hacking. Such measures are used to help compare the extent of the threats that each poses in terms of volumes and frequency. A better preliminary understanding of these measures is helpful when building the evidence base for the costs of cyber crime. The research involved reviewing various published sources (for example, from security vendors, security surveys and threat reports) to determine the nature and quality of the underlying measures currently (as at 2016) available for cyber-dependent crime.

3.6 THREE STEPS TO UNLOCK CYBER SECURITY VALUE

1. Prioritize protecting people-based attacks: Internal risks are also one of the most difficult obstacles that corporate executives face today. With the rise of phishing, ransomware, and disruptive insider attacks, it's more important than ever to foster a security-first community. Accountability is extremely important. To reinforce healthy practices, both within the company and through the broader industry community, training and education are critical. As a result of doing business online, partners, third parties, and partnerships are growing. To collectively protect and defend their activities, organizations should collaborate with these ecosystem partners. People who are interested are not necessarily those who work for a business.

2. Invest to limit information loss and business disruption:Any organization's lifeblood is information, whether it's information about clients, staff, goods, corporate practices, or facilities. As recent privacy laws, such as GDPR and CCPA, impose significant penalties for non-compliance, companies must take responsibility for their sensitive data. Information security is at the core of ethical

corporate practices, and it's essential to avoid business interruption. Using a data-centric approach to security, data loss management systems, and widespread use of cryptographic technology will also help to lower the cost of cybercrime. Enhancing compliance policies around information handling, maintenance, and distribution will help an enterprise transition from harm reduction to secure proprietary procedures when it comes to data loss.

3.7 LET'S SUM UP

In this chapter, we have learned about the cost analysis of cybercrime framework and its various dimensions associated with different stakeholders.

3.8 FURTHER READING

- E. Tyugu, "Artificial intelligence in cyber defense", In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11,2011.
- X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, "Review on the application of Artificial Intelligence in Antivirus Detection System", In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506- 509,2008.
- M Rajesh Kanna, D. Hemapriya and C. Divya," Intelligent Agents For Intrusion Detection System (IAIDS)", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013.
- N. Jaisankar, R. Saravanan, K.Durai Swamy, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009.
- Yu Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure", In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008.
- Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, "Application of Artificial Neural Network in Detection of Probing Attacks", In Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA), 2009

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Provide few examples of cost incurred through cyber crime framework

Government activities

- Drafting and creating new legislation

- Efforts to educate public on new legislation
- Implementation of national awareness raising/protection campaigns

Other

- Cyber-insurance administration
- Consumer credit/identity protection services (for example, CIFAS, a fraud protection organisation)
- Fear/worry about cyber crime
- Collection and compilation of cybercrime statistics

3.10 ACTIVITY

Explain the costs of cybercrime framework and various types of cost.(Word count 2000 to 2500)

Unit 4: CYBER CRIMES: GLOBAL AND INDIAN RESPONSE

4

Unit Structure

4.1 Learning Objectives

4.2 Global perspective of Cyber Crimes

4.3 Country wise Legal Response

4.4 Cyber crimes: An Indian Response

4.5 Nature of Offences and Penalties

4.6 Let's sum up

4.7 Further reading

4.8 Check your progress: Possible answers

4.9 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Global perspective of cyber crimes
- Countrywise legal response
- Nature of offences and penalties in India

4.2 GLOBAL PERSPECTIVE OF CYBER CRIMES

One of the most distinguishing characteristics of cybercrime is that it has a significantly broader reach than typical crime. An illegal act committed in one part of the world may have consequences in another. Because of the scope of cybercrime, the whole planet has effectively become a small town. Another characteristic is that the criminalization of cybercrime and the rise in cybercrime is consistent all over the world. It is likely that a crime is committed in one country but not in another. However, if a person commits a felony, even if it is not a crime in his own country, he can be tried under the laws of another country. For example, if an individual in the United Kingdom sends a virus to a machine in India, he could face legal action in India. As a result, cybercrime has omnipotent property, and as a result, it can have victims anywhere on the planet. It is now important for all those who work in the tech world to have a basic understanding of what constitutes cyber crime in numerous countries around the world.

Since the influence of cyber crime is unbounded, any attempt taken at the national level must be international in scope in order to effectively contain cyber crime and defend the interests of society as a whole. Such circumstances necessitate an interpretation of the global legal approach to cybercrime. All around the globe, innovations and technologies, both positive and disruptive, are happening at breakneck speed. Without foreign collaboration, neither country will be able to keep up with the latest developments in the other. A nation that has been a target of recent cybercrime should be able to alert other countries in advance so that it can prepare its security ahead of time. The aim of this page is to provide a brief description of the main features of numerous world statutes.

4.3 COUNTRYWISE LEGAL RESPONSE

The legal approaches to cybercrime in different parts of the world are complex. Such regulation is also in its infancy. There isn't a single regulation that can be said to encompass all of the requirements of current cyber legislation. Unsolicited calls from telemarketers and others, for example, are supposed to be an assault on a person's right to privacy and liberty, but the Indian IT Act and regulations make no allowance for such an act. The United States, on the other hand, adopted a new law for the reason some 13 years ago, and some European countries have followed suit to protect users from telemarketers and mobile phone providers. Some of the representative legislature efforts made by the various countries across the globe are being discussed here.

The United Kingdom, closely followed by Austria, was the first country to enact laws in the area of cyberspace. *The Computer Misuse Act, 1990*, was passed in the United Kingdom, and it includes penal provisions for cyber criminals. Following that, the nation passed the *Regulation of Investigatory Powers Act, 2000.* Following that, Austria took action in the region, amending its current laws with the passage of the *'Cyber Crime Act, 2001'* to combat cybercrime. In November of 2000, Belgium amended its existing laws and made computer forgery, vandalism, computer theft, and hacking criminal offenses. To control internet operations, China passed the *'Computer Information Network and Internet Security Protection and Management Regulations, 1997,'* but the focus was on national security rather than cybercrime prevention. Certain provisions in Estonia's criminal code apply to cybercrime.

Certain provisions of the German Penal Code refer to offences committed with the assistance of computers and data networks. *'The Criminal Damage Act, 1991'* was passed in Ireland, and it provides specific rules on harm caused on or by a computer device or network. *The Computer Crimes Act, 1997* of Malaysia is devoted specifically to computer-related crimes. Malta passed the *'Electronic Commerce Act, 2001'* to regulate electronic commerce, and Part VII of the Act includes amending rules for 'Computer Misuse' to be introduced into the country's criminal code. The Mauritius Penal Code includes specific laws regulating computer-related offences. To fight cybercrime, the nation passed the *'Information Technology (Miscellaneous Provisions) Act, 1998.'* Aside from these rules, there is the *'The Economic Crime and Anti-Money Laundering Act, 2000,'* which deals with money laundering directly.

Romania's legal framework for cybercrime and other associated illegal activity is satisfactory. Title III is the country's title. The anti-corruption law, as well as Laws No. 676 and 196/2003, regulate "the collection of personal data and the security of privacy in the telecommunications industry" and "the prevention of pornography," respectively. 'Singapore's *Computer Misuse Act, 1998,* is devoted specifically to cybercrime. Related clauses can also be found in the UK's *'The Computer Misuse Act, 1990.'* The United States of America (USA) provides the most comprehensive regulatory framework for dealing with cybercrime. It has enacted a number of laws that have regulations pertaining to the device and network abuse. There are several clauses in the Federal Code as well. Individual states have also passed their own regulations on the matter.

4.4 CYBER CRIMES: AN INDIAN RESPONSE

The Indian Act is based on the model law and governs mainly e-commerce. The Act does not focus its attention on the various forms of cybercrimes. The major issue covered under the provisions of the Act are as follows:

- Establish rules which recognize and validate contracts executed through electronic mediums;
- Covers default rules for contract creation and governance of e-contracts performances;
- Provides the definition and characteristic of valid electronic writing and an original document;
- Contains provisions for the recognition of electronic signatures for legal and commercial purposes;
- Recognizes the admission of computer evidences in courts and arbitration proceedings.

Because of the drastic changes in our lives brought on by emerging media and modern communication systems, the legislation was enacted. Company transactions are increasingly being performed using computers and the internet. Instead of conventional paper papers, the general public and business world are gradually using computers to construct, distribute, and preserve information in electronic form. Electronically encoded information is not only less expensive but also faster to store,

retrieve, and communicate. While citizens were aware of these benefits, they were nevertheless afraid to perform business and transactions online due to a lack of legal structure. Many regulatory requirements have historically accepted only paper-based records and signature-based papers. Since electronic trading was expected to replace paper-based transactions, regulatory reforms to promote e-commerce were desperately needed. In 1996, the United Nations Committee on International Trade Law introduced a Model Law on Electronic Commerce to resolve this urgent need. India, as a signatory, introduced 'The Information and Technology Bill, 1999' in Parliament with the aim of promoting Electronic Governance and e-commerce in the country by way of suitable amendments in the existing laws of the country.

The Act's goals are specified in the Act's declaration and reasons. The way we work has changed dramatically as a result of new networking technologies and emerging media. A change is taking place in the way people do business. Instead of conventional paper records, companies and customers are gradually using computers to construct, distribute, and store information in electronic form. There are many benefits of storing information in an electronic file. It is less costly, easy to store, retrieve, and connect with, and it is faster. Despite these incentives, citizens are afraid to perform business or complete any transaction in an electronic format due to a lack of adequate legal structure.The conditions for legal approval of writings and signatures are the two main roadblocks to promoting electronic commerce and electronic governance. Many regulatory requirements currently presume the presence of paper-based records and documentation, as well as the expectation that these records carry signatures. Traditionally, the law of evidence was focused on written documents and oral testimony. Since electronic trading removes the need for paper-based purchases, regulatory reforms have become an immediate requirement to promote e-commerce. In the last few years, foreign exchange through the medium of e-commerce has evolved exponentially, and many countries have moved from conventional paper-based commerce to e-commerce.

4.5 NATURE OF OFFENCES AND PENALTIES

Although the Act's primary purpose is to promote e-commerce rather than to restrict cyber criminals, it does specify a range of offences and punishments that deal with actions and omissions that come under the scope of cyber crimes. Offences are

dealt with in Chapter XI of the Act, while fines and adjudication are dealt with in Chapter IX. Chapter IX focuses on the following features:

- Regulating conduct in its unique way;
- Civil regulations to be employed by premise rather than criminal;
- The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
- Such adjudicating officers are required to know the law and IT or must have judicial experience;
- Adjudicating officers are vested with the power of civil court;
- The proceedings to be conducted by such adjudicating officers are to be construed as judicial proceedings;
- The quantum of compensation to be calculated at the market rate for loss or sufferings.

- ***Penalty for Damage of Computer, Computer System or Network***

Section 43 of the Information Technology Act, 2000 stipulates a liability to pay damages in the form of compensation not exceeding Rs. One crore to the persons so affected where any person without the permission of the owner or any other person, who is incharge of a computer, computer system or computer network, does any of the following acts:

- accesses or secures access to any device, computer system, or computer network;
- scans, copies, or extracts any data, computer archive, or information from such computer system or computer network, including information or data retained or stored on any disposable storage medium;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system, or computer network;
- causes any device, computer system, computer network, database, or other programs residing in that computer, computer system, or network to be destroyed or caused to be damaged;
- interferes with or causes interference with any device, computer system, or computer network;

- denies or causes a denial of access to any individual authorized to access any computer, computer system, or computer network by any means;
- extends some help to someone in order to allow access to a device, computer system, or computer network in violation of this Act's provisions, guidelines, or regulations;
- interfering with or modifying any device, computer system, or computer network to charge a person's services to the account of another person.

- ***Penalty for Failure of Return, Information, etc.***

Section 44 of the Act mandates such legal formalities, stating that "any person who is required under this Act or any rules or regulations made thereunder to furnish returns, maintain books, accounts, or otherwise comply with any provision of this Act or any rule or regulation made thereunder to furnish returns, maintain books, accounts, or otherwise comply with any provision of this Act or any rule or regulation made thereunder to furnish returns, maintain books, accounts,

- ***Residuary Penalty***

According to Section 45 of the Act, anyone who violates any of the Act's rules or regulations for which no separate penalty has been established is liable to pay a compensation of not more than twenty-five thousand rupees to the person affected by the violation or a penalty of not more than twenty-five thousand rupees to the person affected by the violation.

- ***Offence Relating to Tampering with Computer Source Documents***

The Act's Chapter XI describes such crimes and outlines the penalty for them. Tampering with machine source documents is specified in Section 65.

- ***Offence of Hacking***

The crime of hacking a computer device is described in Section 66. Under the terms of this act, anybody who hacks a computer resource with the intent to trigger or believing that he is liable to cause wrongful loss or injury to the public, or anyone who damages or changes any information residing in a computer resource, diminishes its worth or utility, or affects it injuriously by any way, commits hacking, and anyone who commits hacking faces a sentence of up to three years in jail, plus a fine.

- ***Offence of Obscene Publication in Electronic Form***

Section 67 of the Act makes the publication of information that is obscene in the electronic form an offence. According to this provision, anyone who publishes or transmits or induces to be published in the electronic form any contentthat is lascious or appeals to the prurient interest or whose effect is such that its appears to deprave and corrupt individuals who are likely, given all applicable circumstances, to read, see or hear the matter contained or embodied in it, shall be punishable on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. The section covers cyber crimes such as child pornography existing in the cyberspace.

- ***Offence of Non-compliance of Instructions from Controller***

The Controller of Certifying Authorities are appointed by the central government under the provisions of section 17 of the Act. Under section 68 of the Act, the Controller is empowered to direct a certifying authority, or any employee of such authority by order to take steps or cease carrying out of such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules and any regulation made thereunder. Anyone who fails to comply with such an order is guilty of a crime and faces a sentence of imprisonment for not more than three years or a fine of not more than two lakh rupees, or both.

- ***Offence of Misrepresentation or Suppression of Facts***

According to section 71 of the Act, anyone who makes any misrepresentation to, or conceals any material fact from, the Controller or the Certifying Authority for the purpose of acquiring any license or digital signature certificate, as the case may be, is punishable by imprisonment for a period up to two years, a fine up to one lakh rupees, or both.

- ***Offence of Breach of Confidentiality and Privacy***

According to section 72 of the Act, except otherwise specified in this Act or any other legislation currently in effect, whenever any person has secured access to any electronic record, book, register, correspondence, records, paper, or other material

without the permission of the person concerned and discloses such electronic record, book, register, correspondence, information, document, or other material in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder,

- ***Offence of Publishing Digital Certificate False in Certain Particulars***

Section 73 (1) states that no one can publish or otherwise make a Digital Signature Certificate accessible to anyone with information that the certifying authority specified in the certificate has not issued it, the subscriber mentioned in the certificate has not authorized it, or the certificate has not been revoked or removed, unless the publication is for the purpose of verifying a transaction.

Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years or with a fine which extends to one lakh rupees or with both.

- ***Offence of Publication for Fraudulent Purpose***

According to Section 74 of the Act, anybody who intentionally produces, publishes, or otherwise makes available a digital signature certificate for some fraudulent or unlawful reason faces a sentence of imprisonment of up to two years, a fine of up to one lakh rupees, or both.

4.6 LET'S SUM UP

In this chapter, we have studied the Indian and Global perspective of cybercrimes along with how each country has viewed the same. In furtherance, we saw the nature of offences and penalties of cybercrimes under the Information Technology Act, 2000.

4.7 FURTHER READING

- Cole, E. Advanced Persistent Threat: Understanding the Danger and How to Protect
  Your Organization. Massachusetts: Syngress Is an Imprint of Elsevier, 2013.
- Wood, P., Editor. Symantec Internet Security Threat Report 2014, vol. 19. Mountain
  View, CA: Symantec, 2014.

- Greisiger. Cyber Liability and Data Breach Insurance Claims: A Study of Actual
  Payouts for Covered Data Breaches, 4–5.
- Business Section. “Cyber-Security: White Hats to the Rescue.” In The Economist, New
  York: Print Edition, 2014.
- Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. The Economic Impact of Cyber-Attacks. CRS Report for Congress; Congressional Research Service: The Library of Congress, Washington, DC, RL32331, 2004.

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Which country enacted the first cybercrime law?**

The United Kingdom, closely followed by Austria, was the first country to enact laws in the area of cyberspace.

2. **What does Chapter IX of IT Act, 2000 discuss about?**

Chapter IX focuses on the following features:

- Regulating conduct in its unique way;
- Civil regulations to be employed by premise rather than criminal;
- The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
- Such adjudicating officers are required to know the law and IT or must have judicial experience;
- Adjudicating officers are vested with the power of civil court;
- The proceedings to be conducted by such adjudicating officers are to be construed as judicial proceedings;
- The quantum of compensation to be calculated at the market rate for loss or sufferings.

3. **What’s the objective of the Information and Technology Bill, 1999?**

India, as a signatory, introduced ‘The Information and Technology Bill, 1999’ in Parliament with the aim of promoting Electronic Governance and ecommerce in the country by way of suitable amendments in the existing laws of the country.

4.9 ACTIVITY

Elaborate on countrywise cybercrime laws across the globe along with a few provisions pertaining to it? (3000-3500 words)

Block-3

TYPES OF CYBER CRIMES

Unit 1: FACETS OF CYBER CRIME

1

Unit Structure

1.1 Learning Objectives
1.2 Kinds of cyber crimes
1.3 Crimes committed via Mobile and Wireless Technologies
1.4 Let's sum up
1.5 Further reading
1.6 Check your progress: Possible answers
1.7 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The different kinds of cybercrimes
- Crimes committed through Mobile and wireless technologies

1.2 KINDS OF CYBERCRIMES

a) Cyber Stalking

It is the act of stalking, bullying, or assaulting others by the use of the Internet or a device. This is often done to defame an individual using facebook, social media, instant messenger, web-posting, and other Internet-based mediums that include anonymity. False charges, assaults, sexual harassment of minors, and surveillance are examples of bad behaviour.

b) Child Pornography

It is the possession of a photograph or video of a person (under the age of 18) engaging in sexual activity.

c) Forgery and Counterfeiting

It is the use of a device to forge a document, and counterfeiting is the act of forging a document. With advancements in hardware and software, it is now possible to create a duplicate document that is so similar to the original that the validity of the document cannot be determined without expert judgment.

d) Software Piracy and Crime related IPRs

Software piracy is described as the unauthorized copying and dissemination of software for personal or commercial purposes. It falls in the category of intellectual property theft fraud. Other types of IPR piracy offences include music downloads, video downloads, and so on.

e) Cyber Terrorism

It is described as the use of computer tools to threaten or coerce the government, the civilian community, or any part of the population in order to achieve political or social goals.

f) Phishing

It is a method of obtaining a person's personal and sensitive information via e-mail by impersonating a trustworthy source in electronic correspondence. Identity fraud is the aim of phishing, and sensitive details such as usernames, passwords, and credit card numbers can be used to rob money from a user's account. Vishing is the use of a telephone as a means of committing identity fraud (voice phishing). Sms is a form of phishing in which consumers are enticed by text messages.

g) Computer Vandalism

It is the act of physically damaging computer facilities by the use of coercion or malicious software.

h) Computer Hacking

It is the act of altering computer hardware and software to achieve an objective other than the creator's original purpose. Hacking a computer device can be done for a variety of purposes, ranging from simple displays of technological abilities to locking, altering, or damaging knowledge for social, economic, or political reasons. Now, companies are hiring hackers, or people who specialize in hacking computers, to purposefully break into a company's operating system in order to find and patch security flaws.Hackers can be graded as follows:

- **White Hat:**

White hat hackers are those who break into a system to discover security flaws and warn organizations so that preventative measures can be taken to protect the system from outside hackers. White hat hackers may be paying employees of a company who are hired to discover security flaws, or they can be freelancers who want to prove their worth in this area. Ethical hackers are a common term for them.

- **Black Hat:**

The black hat, in contrast to the white hat, hacks the machine with malicious intent. They could use the mechanism to further social, political, or economic goals. They discover the system's security flaws, retain the files, and manipulate the system for personal or corporate gain until the company whose system has been compromised is aware of the problem and applies security patches. Crackers is a common nickname for them.

- **Grey Hat:**

Grey hat hackers identify vulnerability flaws and flag them to site administrators, offering to patch the problem for a price.

- **Blue Hat:**

A blue hat hacker is someone who works outside of computer technology consultancy companies to bug-test a device before it goes live, searching for exploits to close.

i) Creating and distributing viruses over internet

An organization's business and financial losses may be caused by the transmission of a virus. The cost of restoring the machine, the cost of lost sales through downtime, and the cost of lost opportunities are all included in the loss. If the hacker is discovered, the company will sue him for an amount greater than or equal to the damage he caused.

j) Spamming

Spamming is the practice of sending unsolicited and advertising bulk messages over the internet.When an e-mail satisfies the following conditions, it is considered spam:

- Mass mailing: The e-mail is not sent to a single user, but rather to a vast group of people.
- Anonymity: The person's true identity is unknown.
- Unsolicited: The recipient is not expecting or requesting the e-mail.

These spams not only irritate recipients and overburden the network, but they also waste time and take up precious mailbox memory space.

k) Cross site scripting

It is the act of inserting a malicious client-side script into a legitimate website.The malicious script gets access to cookies and other personal information as soon as the browser executes it, and it sends it to remote servers. This knowledge can now be used to obtain monetary gain or physical access to a device for personal gain.

l) Online Action Fraud

There are several reputable websites that have online auction services. Taking advantage of these websites' reputations, some cybercriminals trick shoppers into

online auction scam schemes, which often result in either overpayment of the goods or the item never being shipped after paying is received.

m) Cyber Squatting

It is the act of reserving the domain names of someone else's trademark with the intention of then selling them to the trademark owner at a higher price.

n) Logic Bombs

Malicious malware has been introduced into legal applications. A particular state sets off the malicious behaviour. If the circumstances remain the same in the future, the malicious operation begins, and depending on the action specified in the malicious code, they either kill or render the device unusable.

o) Web Jacking

A hacker gains access to an organization's website and then blocks or modifies it to serve political, economic, or social goals. Some educational institutes' websites were compromised by Pakistani hackers, and animation with Pakistani flags was flashed on the homepage of these websites. On the occasion of India's Independence Day in 2014, Indian hackers hacked the website of Pakistani railways and blinked the Indian flag on the homepage for several hours.

p) Internet Time Thefts

Hacking an individual's ISP username and password and browsing the internet at his expense is known as Internet Time Theft.

q) Denial of Service Attack

It is a malware attack in which the network is clogged and, in some cases, collapsed as a result of useless traffic entering the network, obstructing legal network traffic.

r) Salami Attack

It's a kind of attack that starts with small steps and builds up to a massive assault. The changes are so minor that they go unnoticed. An example of a salami attack is getting access to an individual's online banking and removing small sums of money that go unnoticed by the owner. Frequently, a default trigger is set in the banking website, and withdrawals below a certain threshold, such as a Rs. 1000 withdrawal, are not registered to the account holders. Withdrawing an amount of Rs. 1000 over a span of time would result in a significant withdrawal.

s) Data Diddling

It is a method of altering data before entering it into a database device. Frequently, the original data is kept until the data has been processed. For e.g., a person's DA, or simple wage, is adjusted in his or her payroll data for pay estimation. The total pay is offset by his real salary in the report after the salary is measured and credited to his account.

t) E-mail Spoofing

It is the method of altering the header information of an e-mail so that the original source is obscured and the e-mail appears to have come from a source other than the original source to the recipient.

1.3 CRIMES COMMITTED VIA MOBILE AND WIRELESS TECHNOLOGIES

When a thing is created, a new invention is made, or something otherwise unknown to humanity is explored, the thing that is invented was almost always achieved with the intention of benefiting mankind and the world's development and prosperity. However, history shows that almost all created has been used for both positive and negative ends, i.e. for both constructive and destructive purposes.We can use several examples to understand this, such as 'Nuclear Energy,' which was discovered with no knowledge by scientists that its most large-scale use in the future will not be as an alternative source of energy for the sake of mankind, but in the manufacture of nuclear bombs, which will cast doubt on humanity's very existence. We can also use the example of the Internet, which was deregulated after it was discovered with no knowledge by scientists that its most large-scale use in the future will not be as an alternative source of energy.However, we can see that it is now almost similarly used for both helpful and negative practices, such as frauds, pornography, extortion, hacking, stalking, and so on.This is also true of wireless technology and the mobile phone scheme, all of which have been widely misappropriated for illicit and disruptive purposes.[27]

[27] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012. p. 569

Mobile phones are at the centre of a quickly spreading crime epidemic, with stolen phones even being used as a form of criminal ‘currency.’ Detection and conviction was often complicated due to the technical complexities of phone theft. As a result, we need additional legislation to address cell phone-related crimes and issues.

a) Phreaking

Phreaking is a slang word for a subculture of people who research, play with, or misuse telephones for the purposes of entertainment or usefulness. The word ‘phreak’ may also refer to the manipulation of a phone device using different audio frequencies. It is often grouped with machine hacking because it is thought to be related. This is referred to as the H/P culture (H for Hacking and P for Phreaking.) The majority of phreakers are between the ages of 12 and 17. Most people stop here, and if the defendant is no longer a juvenile, the sentences will get more serious.

Many Phreaking methods can be applied with small electronic circuits that can be quickly built by hobbyists until the key to their operation is discovered.An early phreak who designed one in a blue enclosure gave it the nickname “blue box” because it was the first circuit to produce the switching tones required to reroute long-distance calls. Other Phreaking circuits were assigned identical names soon after. There have been plenty of other types of ‘boxes’ invented. Modern phreaking often includes making phone calls using a company’s private branch exchange system, especially those accessible via toll-free numbers. Phreakers should not necessarily engage in criminal conduct.In reality, in the programming world, they may be considered a hacker. Phreakers may be more interested in the telecommunications industry, especially the less well-known aspects of telephones.

b) Mobile Phone Theft

Increased rivalry in the mobile telephony market has resulted in competitive tariffs, which has boosted telecom growth and teledensity. At the bottom end of the market, the expense of the phone is most likely the biggest impediment. Despite the fact that this expense has been slowly declining, there is still a price difference between the grey market (which includes stolen/smuggled handsets) and the legal market. Any

steps must be taken to curb this crime of smartphone stealing in order to minimize the unregulated grey market and protect consumer interests.[28]

The theft of mobile phone instruments is becoming a major issue in both countries, and it is a major cause of urban crime and robbery. This is regarded as a significant concern worldwide, and the topic is being investigated in order to find a viable solution. In the United Kingdom, a bill (the Mobile Phones Reprogramming Act 2002) was enacted to prevent handsets from being reprogrammed. Reprogramming would allow for re-use but still making it impossible to track down any phone burglary.Other initiatives, such as the development of a Global Central Equipment Identifying Register (CEIR) in Dublin, Ireland, and a "Mobile Industry Crime Action Forum" comprised of operators, manufacturers, and retailers to combat mobile phone fraud and related issues, are also underway.

The United Kingdom is collecting data on cell phone fraud in the European Union via questionnaire answers. These numerous campaigns, including answers to the EU questionnaire, reveal that tackling the issue of mobile phone fraud requires a variety of concerted efforts.Efforts must be made by a variety of groups, relying on a particular database, administrative processes, and collaboration between manufacturers, network operators, and government agencies. In reality, to address this issue, there is a need for even cooperation among governments. It is possible to classify some of the key factors/agents that have arisen as being relevant for combating cell phone fraud based on an analysis of the attempts being made globally.

c) Use of mobile and wireless technology in Terrorist activities

Terrorists' use of wireless technology and mobile phones, among other things, is one of the most harmful uses of these technologies and phones. Terrorists were able to communicate with their colleagues more quickly than in the past, where connectivity was the most difficult obstacle to overcome in the effective execution of a scheme.Terrorist organizations around the world are now well-equipped with cutting-edge networking devices such as the 'Satellite Phone,' which make communication difficult to track. Advanced telecommunications technologies, a collaboration between foreign mobile communications networks and international financial

[28] Preliminary Consultation Paper on Mobile Phone Theft, Telecom Regulatory Authority of India, New Delhi, January, 2004. also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf

institutions, and a lack of legislation allow “m-payments” to be made anywhere, anywhere, by anybody with a mobile phone.Given the global nature of both terrorism and mobile payments, the m-payment service provider, as well as all those tracking terror finance, should have direct real-time access to an interconnected, tightly tracked registry of all people, organizations, companies, and countries accused of having ties to terrorists.[29]

Terrorists can quickly communicate with their masterminds and collect directions via Sim cards given to bogus accounts. After the card is lost, there is no way for investigators to track their whereabouts.

d) SMS spoofing

SMS spoofing is similar to e-mail spoofing in that it seems to come from a familiar number but is actually spoofed and sent by a malicious user. As an illustration, consider the following. Consider a situation in which a woman receives a text message from her husband’s phone in the middle of the night, instructing her to carry cash because he has been in an accident. She’ll almost certainly search the phone number, and if it’s her husband’s, she’ll run out with cash.If this is her answer, she is most likely unaware of the term “mobile spoofing.” A cyber hacker could give someone a message from someone’s cell phone without ever touching it, and no wireless service provider could claim it was spoofed or faked one, thanks to web-based apps.

1.4 LET’S SUM UP

In this chapter, we have studied the different kinds of cybercrimes such as forgery, phishing, hacking, online auction fraud etc. Further, we also have seen the crimes committed through mobile phones and wireless technologies at the present times.

1.5 FURTHER READING

- Gordon, S., & Ford, R. (2003). Cyberterrorism? Onttrek Dec. 20, 2015 uithttp://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[29] The flip Side - Terrorists use mobile payment systems to transfer money, Available at http://www.mgovworld.org/topstory/the-flip-side-terrorists-use-mobile-payment-systems-to-transfer-money/.

➢ Ranger, S. (2014, June 09). Organized cybercrime groups are now as powerful as nations. Onttrek Dec. 20, 2015 uithttp://www.zdnet.com/organised-cybercrime-groups-are-now-aspowerful-as-nations-7000030323/

➢ Recognize scam or hoax e-mails and websites. (s.j.). Onttrek Sep. 27, 2015 uit https://www.communications.gov.au:

https://www.communications.gov.au/what-wedo/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites available under a Creative Commons Attribution 3.0 International License.

➢ Swain, B. (2009, July). What are malware, viruses, Spyware, and cookies, and what differentiates them ?Onttrek Dec. 20, 2015 uit http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookiesand-what-differentiates-them

1.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is spamming?**

Spamming is the practice of sending unsolicited and advertising bulk messages over the internet.

2. **Who are grey hat hackers?**

Grey hat hackers identify vulnerability flaws and flag them to site administrators, offering to patch the problem for a price.

3. **What is the meaning of phishing?**

It is a method of obtaining a person's personal and sensitive information via e-mail by impersonating a trustworthy source in electronic correspondence.

1.7 ACTIVITY

Explain the different kinds of cybercrimes with examples? (1500 – 2000 words)

Unit 2: CYBER TERRORISM

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Definition of Cyber Terrorism

2.4 Essential ingredients of Cyber Terrorism

2.5 Whether the Threat is real or not?

2.6 Examples and Incidents of Cyber Terrorism

2.7 IT Act & Cyber Terrorism

2.8 Let's sum up

2.9 Further reading

2.10 Check your progress: Possible answers

2.11 Activity

2.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- What is cyber terrorism and its essential ingredients
- Famous incidents of cyber terrorism
- Provisions under IT Act with respect to cyber terrorism

2.1 INTRODUCTION

In today's world, the problem of terrorism is a very difficult question. Terrorist assaults on humans have risen significantly over the past decade. Terrorism has affected everyone from ordinary citizens to the country's statehood. It has been a global threat since the conclusion of the Cold War. The state institutions are unable to deter or monitor terrorist threats against humanity; terrorists killed a vast number of people around the world. The national and foreign fronts took a variety of counter-measures, but they were unsuccessful in preventing the terrorist attack. However, most of these are built in a common pattern that might be effective in a normal terror attack. We now live in a modern world, where computers and the internet play a role and can be a valuable weapon in the hands of terrorists.

Acts of terror have moved beyond the physical world. The computer, computer system and networks are being engaged to bring well-coordinated attacks against Nation States. Even in cyberspace, Nation States have started drawing imaginary lines of control and indulging in proxy wars. Since the acts of cyber warfare finely mesh with cyber-terrorism – it is thus imperative that a Nation-State have a legal framework, which curbs cyber terrorism and strengthens cyber security. Cyber-terrorism requires intensely focused efforts with the aim of committing terrorism. It is a new vulnerability with the potential to do substantial harm. Although we frequently equate terrorism with the loss of life, we do not ignore the significant implications of cyber-terrorism, such as fear and manipulation.[30]

In the long term, a continuous and focused terrorist program against a nation has the potential to degrade it. Given the broad spectrum of economic, environmental, and even psychological implications that such a campaign might have, cyber-terrorism will continue to be a major threat in the future. Most countries in the world today

[30] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

depend heavily on technology. An attacker's perfect tactic would be to land a heavy blow on such a crucial backbone. The United Nations' telecommunications department has given an alert that the next world war could well take place in cyberspace. It should come as no surprise that this is the case. Attacks on enemy installations or facilities have commonly been used in wars to deal a crushing blow and gain the upper hand. Given the modern world's absolute reliance on technology, it would theoretically make an excellent target in the event of a war.[31]

Cyber terrorism has arisen as a major threat to the global community, as terrorists use it to distribute fake messages in favour of political and religious agendas. The concept "cyber terrorism" is comparatively new, having been invented by tech genius Barry C. Collin.[32] The term cyber terrorism is a mixture of cyberspace and terrorism, and there is no widely agreed concept of cyber terrorism.When it comes to describing the word cyber terrorism, each academic or theorist in the field has a particular viewpoint. The definition of cyber terrorism in this analysis is split into two categories: intent-based and effect-based.It refers to attacks on the country's servers, networks, and network grids, which rely heavily on networks and cause havoc or terror among its people.

2.3 DEFINITION OF CYBER TERRORISM

The concept of cyber terrorism necessitates a broad description, since the nature of the crime necessitates it. Since the essence of "cyberspace" is such that new forms and tools appear on a daily basis, it is not prudent to confine the concept to a formula or pigeonhole. In fact, the judiciary's first duty should be to define the term as widely as possible in order to prosecute criminals severely, enabling the government to fight the evil of cyber terrorism.[33]

There have been some attempts to define cyber terrorism precisely. In May 2000, Dorothy Denning, a computer science professor, presented an admirably unambiguous definition before the House Armed Services Committee: "Cyber crime is where cyberspace and terrorism intersect. It refers to illegal attacks and threats of

[31] Ibid.
[32] Barry Collin, "The Future of Cyber Terrorism," Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, the University of Illinois at Chicago, 1996.
[33] http://www.naavi.org/cl_editorial_04/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm

attacks on computers, networks, and the information stored on them that are carried out to intimidate or coerce a government or its citizens in the pursuit of political or social goals. In addition, for an attack to be classified as cyber terrorism, it must result in violence against people or property, or at the very least cause enough harm to cause fear. Attacks that result in death or bodily injury, explosions, or significant financial loss are examples. Depending on the impact, serious attacks against critical infrastructures could be considered acts of cyber terrorism. Attacks that disrupt non-essential services or are primarily a financial burden would not."[34]

According to FBI "Cyber-terrorism is a criminal act that uses computers and telecommunications capabilities to perpetrate abuse, damage, and/or service interruption in order to instill fear in a community by creating doubt and uncertainty, with the intention of persuading the government or populace to obey a series of laws."[35]

Since the terms cyber crime and cyber terrorism are not synonymous, we cannot assume that any cyber crime is indeed a form of cyber terrorism. To define cybercrime as cyber terrorism, we must first decide if it is motivated by political or ideological motivations. In the current situation, the terrorist organization's objective is to use computers and networks to disrupt the nation's communication, telecommunications, transportation, and financial networks in order to instil fear in the minds of the population, as any country in the world is highly dependent on technology. Terrorists are using computers and networking to carry out illicit activities, as demonstrated by recent attacks in India and across the globe.

2.4 ESSENTIAL INGREDIENTS OF CYBER TERRORISM

Cyber terrorism as an offence exists in three forms. Essential ingredients of these three forms of cyber terrorism are:

Form I:

1. An intention to threaten the unity, integrity, security or sovereignty of India or to strike terror, and

[34] http://www.usip.org/sites/default/files/sr119.pdf
[35] H. M. Hendershot, 'Cybercrime 2003 – Terrorists' Activity in Cyberspace and also at http://www.ijiee.org/papers/126-I149.pdf

2. Causing or likely to cause (i) death or injuries to persons,[36] or (ii) damage or destruction of property, or (iii) damage or disruption of supplies or services essential to the life of the community, or (iv) disruption of or affecting the critical information infrastructure, as specified in Section 70 of the IT Act 2000, by any of the following acts:

a) Denying or causing the denial of access to any person authorized to access computer resource; or
b) Attempting to penetrate or accessing a computer resource without authorization or exceeding authorization or exceeding authorized access; or
c) Introducing or causing to introduce any computer contaminant.

OR

Form II:

1. Knowingly or intentionally penetrating or accessing a computer resource without authorisation or exceeding authorized access, and
2. Obtaining access to restricted information, data or computer database which is restricted for reasons of the security of the State or foreign relations.

OR

Form III:

1. Knowingly or intentionally penetrating or accessing a computer resource without authorization or exceeding authorized access, and
2. Obtaining access to restricted information, data or computer database,
3. With reasons to believe that such restricted information, data or computer database may cause or likely to cause injury to: (i) the interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or (ii) in relation to contempt of court, (iii) defamation, or (iv) incitement to an offence, or (v) the advantage of any foreign nation, group of individuals or otherwise.

As evident from the above discussion, the definition of cyber terrorism is to be seen from both State's as well as its subjects' (citizens) perspective. The scope of cyber terrorism has been made very exhaustive. It takes into account both '*cause-and-*

[36] Cyber terror acts may include causing disruption to nuclear reactors, power grids, dams, aviation, railways etc., which may result into death or injuries to a large number of people.

effect' of cyber terrorism (and related activities). Now the question is whether Section 66F could be misused? Answer lies in how the law enforcement agencies and the Courts would view facts and circumstances in a given case and accords it a status of cyber terrorism. For example, the challenge before the Court would be to distinguish whether an offence of defamation could reasonably be covered under Section 499 of IPC or it requires Section 66F of the IT Act? Under Section 499, defamation is with respect to any person, and the word *'person'* does not include a State, whereas Section 66F implies *'defamation of State'*.[37] This section requires strict interpretation and not liberal interpretation.

Moreover, in view of terrorists' activities increasingly being done by foreign mercenaries, it would be obligatory to read Section 66F along with Section 75 of the Act.

2.5 WHETHER THE THREAT IS REAL OR NOT?

The challenges faced by cyber terrorism has piqued the attention of the media, the IT industry, companies, the defence industry, policymakers, and experts from a number of fields, who have popularized a scenario in which cyber terrorists hack into computers that control dams or air traffic control networks, wreaking havoc and endangering not only millions of lives but also national security.[38]

How serious is the danger faced by cyber terrorism? Since the majority of critical infrastructure in today's world is linked via computers, the threat of cyber terrorism is very real. Cyber criminals can obtain access to classified information and the activity of vital resources with the aid of hackers, undermining or at the very least crippling the security, banking, and service sectors of advanced economies.[39]

Our communities' rising dependence on computers and the internet has created a new category of weakness, allowing attackers to approach targets that would normally be impenetrable, such as national security and air traffic control systems. The more technologically advanced a nation is, the more vulnerable its technology is

[37] Krishnan v. Krishnaveni, AIR 1997 SC 987: 1997 AIR SCW 950: 1997 Cr LJ 1519.

[38] Gabriel Weimann, Cyber terrorism: How Real Is the Threat? Special Report No.119, United States Institute of Peace, December, 2004.also at https://thepeacemission2013.files.wordpress.com/2013/03/study-guide-united-nations-counter-terrorism-committee.pdf

[39] Terror on the Internet: The New Arena, the New Challenges USIP Press Books, 2006. also at http://www.usip.org/sites/default/files/sr119.pdf

to cyber threats. As a consequence, there is cause to be worried about the possibility of cyber terrorism.

While cybercrime is on the rise, there has been no cyber terrorist attack on Indian public buildings, highway networks, nuclear power plants, power grids, or other vital national infrastructure machinery. Cyber attacks are common, but they have never been carried out by terrorists or attempted to do the type of harm that can be called cyber terrorism.

2.6 EXAMPLES AND INCIDENTS OF CYBER TERRORISM

The following is a list of events that have caused difficulties for countries or may be identified as terrorist acts by terrorist organisations using information technology around the world:

1. ***Cyber attacks in Middle East***

With tensions between neighbouring countries at an all-time peak, pro-Palestinian and pro-Israel cyber groups have mounted an offensive against websites and postal systems used by political sectors that the opposing groups support. The attacks were confirmed to US officials by the NIPC (National Infrastructure Protection Center) in October of 2000. The threats involved a barrage of e-mail floods, denial-of-service attacks, and Ping flooding against sites belonging to Hamas and Hezbollah, as well as the Israeli Foreign Ministry and Israeli Security Forces.[40]

2. ***India and Pakistan Conflict***

Pro-Pakistan cyber-terrorists and recruited hackers started to threaten India's Internet Population as tensions between the neighbouring regions of India and Pakistan over Kashmir rose. It is suspected that Pakistani sympathizers started distributing lies and attacks against Indian Internet-based populations shortly before and after the September 11thattacks. G-Force and Doctor Nuker have defaced or interrupted service to many big Indian institutions with political links, including the Zee TV Network, the India Institute of Science, and the Bhabha Atomic Research

[40] "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

Center. Pakistani Hackerz Club also went so far as to attack the US Air Force Computing Environment and the Department of Energy's website.[41]

3. Retribution by China

The bombing of a Chinese embassy in Yugoslavia by American bombers in May 1999 triggered a major website defacement and e-mail bombardment attack on American companies and agencies. The attacks were carried out by pro-China hackers and political parties in order to gain support for the Chinese cause. The White House website, as well as the US Departments of Energy and Interior, and the National Park Service, were all attacked and had their websites defaced. Continuous e-mail bombing took the sites down for three days. Since the attack was sporadic and short, and only a limited number of US pages were infected, the results may have been much worse.[42]

4. Cyber attack by Tamil Tigers

With surges of violence in Sri Lanka over many years, cyber-space attacks were the next focus in 1998. The Tamil Tigers, a militant resistance group, sent more than 800 e-mails per day to Sri Lankan embassies. This was done over the course of two weeks. "We are the Internet Black Tigers, and we are doing this to interrupt your communications," said the e-mail address that started the attack. Local Intelligence officials were sent to investigate after the communications caused such extensive damage. The attack was the first recorded attack on a computer device in Sri Lanka by terrorists, according to the authorities.[43]

5. Yugoslavia Conflict

NATO web servers[44] were exposed to persistent attacks by hackers hired by the Yugoslav military as NATO air strikes struck the Former Republic of Yugoslavia in Kosovo and Serbia. All of NATO's 100 servers were exposed to "ping overload,"

---

[41] "Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

[42] Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

[43] Cyber Terrorism – "Testimony before the Special Oversight Panel oil Terrorism"- Dorothy E. Denning - May 23, 2000. also at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931

[44] The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party.

DDoS threats, and a barrage of thousands of e-mails, many of which contained viruses. The attacks on NATO servers were timed to coincide with various website defacements of American military, government, and commercial pages by Yugoslav sympathizers from Serbia, Russia, and China. The NATO communications system is seriously damaged as a result of these attacks.

6. Cyber attack on Estonia

Russia conducted a cyber-attack on Estonia, a tiny Baltic republic. Russian indignation has arisen after the Baltic state's government agreed to strip a war memorial to the Red Army from a square in Tallinn's capital. Demonstrations and even protests were organized as a result. But then something unusual happened: the whole world was exposed to a barrage of cyber-warfare, which made government ministries, political parties, banks, and newspapers unavailable. Cybercriminals' tactics, such as vast remotely managed networks of hacked devices, were used to cripple crucial government systems. NATO has dispatched its top cyber-terrorism experts to Tallinn, leaving Western democracies unprepared for the repercussions of such an attack. "We've been blessed to survive this," the Estonian defence ministry said. When a missile strikes an airport, a bank, or state facilities, it is obviously fighting, so what do you call it when the same outcome is obtained by computers? Is that a war situation? There are problems that need to be addressed."Estonia has, unsurprisingly, accused Russia, which, if real, would make this the first cyber attack on another sovereign state. The Estonian attacks were more likely the result of a single angry young Russian hacker than some kind of Kremlin-sponsored blitz. In either case, the consequences are extreme.[45]

7. Attack on Indian Parliament

On December 13th, 2001, a cyber-attack was launched against the Indian Parliament. To accomplish their target, the attackers used cutting-edge technologies and committed forgery. They faked the gate pass and downloaded the official Ministry of Home Affairs emblem, other records, and the architecture of the Parliament building in preparation for the attack. Police uncovered a laptop belonging to the key criminals, Mohammed Afzal and Shaukat Hussain Guru. The police found that they had accessed the internet via Internet Service Providers

[45] See "Attack of the cyber terrorists" by MICHAEL HANLON Available at: http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html

located in Pakistan (ISP).In addition, the investigation officers uncovered the incoming and outgoing mobile phone numbers of deceased terrorists, as well as a satellite link with the cell phone of a deceased terrorist.[46]

8. Sony PlayStation Network, Microsoft's Xbox Live network case

In this situation, the workers' and their families' personal details were leaked in 2014. Owing to the leak of film, the corporation has lost sales, confidential staff details such as compensation and social security numbers have been released, and executive e-mails have been made public. The Lizard Squad, a self-described cyber-terrorist group, coordinated the attack. Then they conducted a huge DDoS assault against Sony's PlayStation Network and Microsoft's Xbox Live networks. They followed up these disruptions with an assault on the Tor Project, a network of virtual tunnels that helps individuals and organisations to enhance their privacy and protection on the Internet, and then North Korea targeted the network infrastructure, forcing the network to go offline for nearly ten hours, affecting millions of people. As a consequence, many people assumed it is an act of the US government. However, they succeed in instilling fears in customers' minds about buying goods and in the public's view of multinational corporations. The motive behind these cyber terrorism attacks is the collateral harm that is involved, as well as the apparent diplomatic links that we see in so many attacks. "Cyber-terrorism is probably one of the biggest challenges facing the United States today," according to US President Barack Obama. Unfortunately, the attacks are not only here to linger, but with today's total dependence on the Internet, they are also likely to get even more serious."[47]

2.7 IT ACT & CYBER TERRORISM

In today's world, the fastest way to attack a nation is through a cyber network. Since India now heavily relies on computers and information technology, the effect of a cyber assault on Indian infrastructure and connectivity would be tremendous.

In order to fight cybercrime, a collection of creative laws and global norms is needed. The computer/Internet is shaping the process of information formation and

[46] Sayantan Chakravarty, "Parliament attack well-planned operation of Pakistan-backed terror outfits, evidence shows", India Today, December 31st 2001.

[47] See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/

distribution, as well as redefining the networking process by deeper transmission. With caution and attention, a delicate line between terrorism and law enforcement should be reached. As a result, the Information Technology Act, 2000 was enacted to prosecute cyber criminals.

Previously, there was no clear clause in the IT Act, 2000 that dealt directly with cyber terrorism; as a result, the Information Technology (Amendment) Act, 2008 incorporated a new section 66F. In light of the growing terrorist attacks in India and neighbouring countries, the IT Amendment Act of 2008 is a welcome move.

Section 66F is a combination of Section 66 and Section 70 of the IT Act, 2000.[48] What separates Section 66F from other sections is the degree and nature of the offence. If using a sliding scale approach to measure the gravity of the offence, Section 66 is at one end of this spectrum, whereas Section 66F is at the other end of the spectrum.

Penalty	Section 66	Section 70	Section 66F
Imprisonment Term	May extend to three years	May extend to ten years	May extend to imprisonment for life

The strategy of "Counter strike by offensive Defence" may be used to deter cyber terrorism. The principle of counter-strike by proactive security predicts that information technologies can be implemented and used to achieve acceptable and legalized crippling and relatively disruptive results. Any of the steps introduced totally uninstall the offending device, while others merely disable it for the time being by locking it down or rendering it temporarily non-functional. Not only must the equipment used be secure and efficient, but it must also be "ethical and law-abiding." A counter-measure that is not very accurate and law-abiding would be a worse treatment than the epidemic, and therefore should be prevented. For example, if a virus is transmitted by the use of a public server, the real and lawful users would be harassed unfairly, and they will be refused facilities to which they are otherwise entitled. As a consequence, the counter-measure must be job-specific and not disproportionate to the accident being discussed.[49]

[48] Section 69 and 69A are preventive sections and hence not included.

[49] Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer Crime Research Center, March 10, 2006.

The threat of cyber attacks remains “imminent,” according to Pavan Duggal, and the country lacks an institutionalized framework to deal with the threat. “The latest DRDO breach was a textbook case of cyber war attack rather than simple hacking,” he added. It was a cyber-attack on India’s vital data networks. The Indian cyber law does not cover cyber warfare as a phenomenon. Clearly, India’s cyber security is out of line with the demands of the real world.”[50]

India has seen an uptick in cyber terrorist attacks in recent years, with government agencies, especially defence institutions, being attacked. In India, the following cases of cyber terrorism have been identified.

1. In revenge for suspected Internet censorship, the hacker collective ‘Anonymous’ initiated a campaign of Distributed Denial of Service (DDoS) attacks against a number of government websites in 2012.
2. Algerian hackers had targeted the DRDO, the Prime Minister’s Office, and a number of other government departments’ websites in 2012.
3. Hackers and militant groups from Pakistan are rising their attacks on Indian websites, introducing a new layer to the continuing war in Jammu and Kashmir. GForce, an online hacker collective whose founders yell slogans critical of India and its claim to Kashmir, has confessed to breaking into high-security data networks run by the Indian government, including the Bhabha Atomic Research Center’s.
4. In March 2016, the Indian Infrastructure was targeted by Al Qaeda, a militant group that reportedly hacked a microsite of the Indian Railways’ Rail net website to display its sinister scope for the first time. The hacked page of the Central Railway’s Personnel Department’s Bhusawal division, which was part of a large intranet created for the department’s administrative needs, was replaced by a message from Al Qaeda’s South Asia leader, Maulana Aasim Umar, urging all Indian Muslims to join Jihad.[51]

In the arsenal of criminals, information technology becomes a basic weapon.They use computers and networks to communicate in secret with their agents all over the world, preventing capture by law enforcement. The main cyber terrorist attacks in India include the Ayodhya incident, the Mumbai attack in 2006, the defacement of

[50] http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274

[51] http://www.ndtv.com/india-news/al-qaeda-hacks-into-indian-railways-website-leaves-message-to-join-jihad-1283023

Indian military sites in India by hackers in July 2005, the attack on the American Center in Kolkata, and the Pathankot Terrorist Attack, among others.

According to Prashant Mali, a cyber law and cyber security specialist, “the threat environment remains very dangerous, and India is now waking to the global threat of cyber warfare.” Our data protection remains inadequate due to a lack of or insufficient public knowledge. Despite the fact that NTRO and DRDO have been charged with cyber offensive jobs, only time can say how successful these organizations are.”

“The threat environment has changed drastically in the last few years,” said Shantanu Ghosh, vice president of India Product Operations at Symantec Corporation, which developed Norton Antivirus. Attackers’ motive has changed from popularity to profit, and ransomware has become a profitable illegal business model worth billions of dollars. We’ve now joined the third big change in the threat environment, which is one of cyber-espionage and cyber-sabotage.”

2.8 LET’S SUM UP

In this chapter, we have studied how cyber terrorism has been defined by various research scholars along with its essential ingredients. Furthermore, we saw the famous incidents of cyber terrorism across the globe and ended the discussion with the legal framework of cyber terrorism under IT Act.

2.9 FURTHER READING

- Babak Akhgar, Andrew Staniforth, and Francesca Bosco. 2014.Cyber Crime and Cyber Terrorism Investigator’s Handbook (1st. ed.). Syngress Publishing.
- See “Is Cyber-Terrorism the New Normal?” Available athttp://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/
- Robert W. Taylor, Eric J. Fritsch, Michael R. Saylor, and William L. Tafoya. 2018. Cyber Crime and Cyber Terrorism (4th Edition)(4th. ed.). Pearson.
- Joseph F. Gustin. 2004.Cyber Terrorism: A Guide for Facility Managers. The Fairmont Press, Inc., USA.

2.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber terrorism?**

Cyber-terrorism is a criminal act that uses computers and telecommunications capabilities to perpetrate abuse, damage, and/or service interruption in order to instill fear in a community by creating doubt and uncertainty, with the intention of persuading the government or populace to obey a series of laws.

2. **Which provision was introduced under the IT Act to combat cyber terrorism and when?**

Previously, there was no clear clause in the IT Act, 2000 that dealt directly with cyber terrorism; as a result, the Information Technology (Amendment) Act, 2008 incorporated a new section 66F. In light of the growing terrorist attacks in India and neighbouring countries, the IT Amendment Act of 2008 is a welcome move.

3. **Describe the cyber attack by tamil tigers?**

With surges of violence in Sri Lanka over many years, cyber-space attacks were the next focus in 1998. The Tamil Tigers, a militant resistance group, sent more than 800 e-mails per day to Sri Lankan embassies. This was done over the course of two weeks. "We are the Internet Black Tigers, and we are doing this to interrupt your communications," said the e-mail address that started the attack. Local Intelligence officials were sent to investigate after the communications caused such extensive damage. The attack was the first recorded attack on a computer device in Sri Lanka by terrorists, according to the authorities.

2.11 ACTIVITY

Elaborate on the famous incidents of cyber terrorism across the globe along with provisions enacted in IT Act to combat the same. (1500-2000 words)

Unit 3: CYBER PORNOGRAPHY

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Test of Obscenity and Pornography

3.4 IT Act and Pornography

3.5 Combating Child Pornography

3.6 Obscenity and Freedom of Speech and Expression

3.7 Let's sum up

3.8 Further reading

3.9 Check your progress: Possible answers

3.10 Activity

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- The meaning of cyber and child pornography
- Test of obscenity and pornography
- Obscenity and Freedom of speech and expression

3.2INTRODUCTION

The expression' pornography,' derives from the Greek terms 'porne' and 'graphein,' refers to any piece of art or literature that deals with sex and sexual themes or writing about prostitutes. It is difficult to describe the term pornography, as there is no clear legal meaning since each country has its own customs and practices. Pornography is legal in some countries, but it is immoral and punishable in others.

In simple words, cyber pornography is the act of using the internet to create, view, upload, import, or publish pornography or pornographic materials. Traditional pornographic content has been increasingly replaced by online/digital pornographic content with the rise of cyberspace.There is no legal or clear definition of pornography. The response of culture, traditions, and principles to pornographic material defines the concept of pornography.

The lack of a consistent definition of pornography is due to the fact that there is no common standard of culture and ethics in the world, nor are there universal rules that describe pornography. Obscenity and pornography are described differently in various countries and at different times. The words obscenity and pornography are separate, but they are related. The same content that is forbidden in certain countries may be permissible in others.The word pornography is not specified in Indian law, and it is not dealt with.

The advent of the internet to the world has resulted in a new age in the pornography industry. The pornography industry has learned that the internet is the best tool for disseminating pornographic content around the world. According to a 2010 internet filter analysis survey, there are 4.2 million websites worldwide that sell pornographic content. Every day, 68 million searches are made on search engines, and 72 million

people visit adult websites each month around the world.42.7 percent of all internet users watch sexual videos on the internet.[52]

DVDs and videotapes became the most common means of spreading pornography in the early years, or before the internet was readily available.However, after the internet was made accessible to the general public, it soon became the most common avenue for people to view pornography from the privacy of their own homes. A person who may not have access to pornographic content due to social pressure or embarrassment can now freely view pictures or videos on the internet.Greater access to pornography was made possible by the advent of pornography websites that provided images, video clips, and streaming videos, including live web cam access. Over the internet, information technology has made it possible to produce and publish obscene materials; for example, content can be distributed all over the world in seconds, and geographical barriers that historically prohibited international publications from accessing local jurisdictions have vanished.[53]

3.3 TEST OF OBSCENITY AND PORNOGRAPHY

To comprehend the gravity and influence of pornography and obscenity on culture, we must first comprehend these words in their broadest context. The word *'pornography'* has not been legally defined.

The issue of obscenity has always been a complex one as it involves other related issues like decency and morality. It is difficult to judge obscenity in isolation using straitjacket principles. It needs a wider perspective. For example, a depiction of a nude body form is indecent and vulgar for some, but for some, it is an artistic expression to be savoured by one and all. When such a dichotomy exists, it is important that a holistic view should be undertaken as any narrow interpretation of statutes may lead to a miscarriage of justice. It would be more if one were dealing with the vexatious question of *'cyber obscenity'*. Believing and interpreting that *'cyber obscenity'* is an extension of *'physical obscenity'* would be fallacious.

[52] http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html
[53] Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

In the case of *Regina vs Hicklin*,[54] the test of obscenity was first described as the propensity "to deprave and corrupt those whose minds are open to certain forces and into whose hands a publication of this nature may fall," with the assumption that this test will only extend to anisolated passage of the work.

The Supreme Court of the United States in *Miller vs California*[55] released a seminal opinion that established the fundamental principles and three-point tests for evaluating obscenity in work, namely:

1. That the ordinary individual, following contemporary "cultural norms," will find that the work, as a whole, appeals to the prurient interest.
2. That the work illustrates or portrays sexual activity or excretory activities in an objectionable fashion, as described by relevant state or applicable law.
3. Whether the work has serious literary, cultural, political, or science merit as a whole.

Prior to *Miller vs United States*, the Supreme Court of the United States ruled in a landmark case, *Roth vs United States*,[56] that "obscene content was not covered by the First Amendment and should be governed by the States rather than by a single, Federal standard and also a new judicial standard for determining obscenity that invoked the common person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeal to prurient interest."

The Supreme Court went on to state that "to assess if obscenity is derived, we need to consider the following five-part structure:

1. The perspective of the evaluation was from the viewpoint of a man of ordinary prudence.
2. To assess obscenity, societal principles of acceptability were to be included.
3. Obscenity regulations can only extend to works with a particular theme.
4. A work had to be presented in its entirety in order to be judged for obscenity.
5. An obscene work was one that aimed to excited individuals' prurient interest."

[54] Regina vs. Hicklin [1868] LR 3 QB 360
[55] Miller vs. California, 413 US 15(1973)
[56] Roth vs United States, 354 US 476 (1957)

In the leading case of *Ranjeet D. Udeshi vs State of Maharashtra,*[57] the Supreme Court did not use the miller test and instead adopted the Hicklin's Test.The Supreme Court determined several questions related to obscenity. The Supreme Court does not believe obscenity to be a nebulous word, but rather a well-defined term, even though people have different opinions of what is and is not obscene. "In evaluating a work, emphasis should not be put on a word here and a word there, or a passage here and a passage there," the Supreme Court ruled.Though the whole work must be regarded, the pornographic content must be investigated separately to assess if it is so heinous and its obscenity so defined that it is liable to deprave and degrade all whose minds are sensitive to such influences. In this context, it is important not to ignore contemporary society's interests, especially the effect of the contested book on it. When obscenity and art are merged, the art must take precedence over the obscenity, otherwise the obscenity must be so small and trivial that it has little impact and may be ignored.The compromise between "freedom of speech and expression" and "public decency or morals" must be maintained; but, where the latter is significantly abused, the former must surrender."

The Court, on the other hand, warned that treating of sex and nudity in art and literature alone cannot be considered evidence of obscenity. "It is not appropriate to have the angels and saints of Michelangelo wear breeches until they can be viewed," the Court said. If the stringent test of treating sex as the minimum component is adopted, hardly any contemporary writer of fiction can avoid the fate Lawrence did. Part of the bookshops would close, and the other half would specialize in moral and religious literature."

In the said case, the Supreme Court held that "It makes the court the judge of obscenity in relation to an impugned book etc. and lays stress on the potentiality of the impugned item to deprave and corrupt by unethical influences." It will still be a matter for each case to decide, and it does not compel a negative judgment in any case."

The Supreme Court ruled in *Samresh Bose vs Amal Mitra,*[58] that "a lewd writing is not actually obscene." Vulgarity elicits emotions of shame and revulsion, as well as boredom, but it has little effect on the morality of any reader of the books, while obscenity has the power to deprave and degrade those whose minds are sensitive to

[57] Ranjeet D. Udeshi v. State of Maharashtra, AIR 1965 SC 881
[58] Samresh Bose v. Amal Mitra, AIR 1986 SC 967

such unethical influences."The Court differentiated between vulgarity and obscenity in this case, and further noted that when ruling on obscenity, "the Judge should put himself in the role of a reader of any age group into whose hands the book is likely to fall and should try to understand what sort of potential effect the book is likely to have in the minds of the readers."

The Supreme Court of India presently adopts the *Community Standards Test* as a measure of detecting obscene content. In *Aveek Sarkar vs State of West Bengal*[59], the facts of the case revealed that a German magazine published an article about a tennis player picturing him naked with his fiancé as a stand against racism and to show that love champions over everything. The Supreme Court found the respondents innocent of the charges levied against them and held that in a situation like this Hicklin's test cannot be used and the only measure to be implemented is the community standards test; and it further stated that the photograph must be viewed in the context of the message which the photograph appears to convey, and not in isolation. The Supreme Court further instructed that a more adaptive community standards test must be applied for a continuously evolving society like India.

3.4 IT ACT AND PORNOGRAPHY

Section 67 of the IT Act, 2000 deals with obscenity and pornographic content on internet. Similarly, Section 292 of the Indian Penal Code, 1860 deal with the issue of obscenity.

According to Section 67, obscene content in electronic form must be investigated individually to determine if it is so gross and its obscenity so defined that it is likely to deprave and degrade those whose minds are vulnerable to such effects and into whose hands the obscene material in electronic form is likely to fall.

Critically speaking, the said provision, like Section 292(1) of IPC, does not make knowledge of obscenity an ingredient of the offence. Thus to escape criminal charges, one has to prove his lack of knowledge of publication or transmission of obscene information in electronic form. Moreover, though publication or transmission of obscene information may be illegal but mere possession, browsing or surfing through obscene content is not an illegal activity.

[59] (2014) 4 SCC257

It should be noted that under no circumstances any offence related to obscenity in electronic form should be tried under Section 292 of IPC as Section 81 of the IT Act, 2000 states that the Act will have an overriding effect:

'The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force'.

Moreover, the punishment provision under Section 67 of the Act is far more stringent, i.e., *'The offender/s shall be sentenced with imprisonment of either description for a period not exceeding three years and a fine not exceeding five lakh rupees on the first arrest, and with imprisonment of either description for a term not exceeding five years and a fine not exceeding ten lakh rupees on the second or subsequent conviction'* at least monetary wise, than what is being given under Section 292 of IPC. Thus any attempt to use Section 292 IPC for publishing or transmitting of information, which is obscene in electronic form instead of Section 67 of the Act would create unnecessary confusion and may also result in miscarriage of justice.

Section 67 of the IT Act of 2000 is identical to Section 292 of IPC.In the case of *Ranjit D. Udeshi v. State of Maharashtra*, the Court ruled that, unlike other clauses that contain terms like "knowingly" or "negligently," this one does not.As a consequence, mens rea becomes a requirement for maintaining remorse. The offence is not made more egregious by the fact that the perpetrator is aware of obscenity. The Prosecution should not have to assert anything that the statute does not demand.The challenge in collecting legal proof that the defendant was aware of the offence has made the liability strict.The lack of such information can be considered a mitigating cause, but it does not exclude the situation from the clause. If we refer the *Ranjit D. Udeshi case* to Section 67 of the IT Act, 2000, we can infer that the mere publishing and dissemination of indecent content is a crime, regardless of the offender's mental state.This, though, cannot be a common law that applies to all.[60]

3.5 COMBATING CHILD PORNOGRAPHY

In today's world, children, especially teenagers, want to explore everything on the knowledge highway. Today's children have access to the internet and computers at

[60] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012, p. 440

home, and they are expected to use the internet and computers as part of their studies. They are vulnerable to the perceived risks of the internet and they have access to computers and the internet.Children are occasionally involved in sexuality and sexually suggestive content. The parents have little influence over their children, and the children are occupied with exploring the internet and other media in order to satisfy their desires through online access.Children's interests are fulfilled by sex–offenders who take advantage of the situation. At this age, the infant is unable to comprehend or consider the possible risk of these experiences. Abusers use the internet widely to sexually assault minors all around the world.Since the internet has become a household item in India, children have become vulnerable to cyber crime. Paedophiles are committing acts of abuse against children.

In the physical world, parents are mindful of the risks and educate their children about how to prevent or cope with difficulties by following simple instructions. However, when it comes to cybercrime or online-related crime, most parents are unaware of the concerns or risks presented by the different resources provided on the internet. Paedophiles take advantage of these circumstances by luring children and gaining their trust, and manipulating them when their parents or teachers do not warn them of what is wrong or right on the internet.

The Information Technology Act, 2000 does not have any clear rules on child pornography, but later, the Information Technology Amendment Act, 2008 introduced a new Section 67B.

The said provision criminalizes all kinds of online child pornography. The term online refers to publishing or transmitting of material depicting children in the sexually explicit act, etc., in electronic form. Under the said section, five instances of online child pornography have been criminalized:

a) Publishing or transmitting or causing to publish or transmit material in any electronic form which depicts children engaged in sexually explicit act or conduct;
b) Creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing material in any electronic form depicting children in obscene or indecent or sexually explicit manner;
c) Cultivating, enticing or inducing children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource;

d) Facilitating abusing children online, and
e) Recording in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

Although under Section 67B, five instances of online child pornography have been criminalized, but it is obligatory to note that clauses (a) and (e) are generic in nature, whereas clauses (b), (c) and (d) are specific.

In the case of *U.S. vs Joseph C. Bledsoe,*[61]the defendant was convicted for knowingly publishing a notice over the Internet offering to exchange child pornography on violation of 18 U.S.C. § 2251(d). The defendant appealed his conviction and sentence. The U.S. Court of Appeals for the Fourth Circuit affirmed the conviction and sentence.

Similarly, in *U.S. vs Philip M. Sebolt,*[62] the accused was convicted for using computer to possess, transmit, advertise child pornography in violation of 12 U.S.C. §§ 2252A(a)(1), 2251(d)(1)(A). Also, in *U.S. vs Michael Shawn McCourt,*[63] the defendant was convicted for attempted distribution and attempted receipt of child pornography over the Internet and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (4).

3.6 OBSCENITY AND FREEDOM OF SPEECH AND EXPRESSION

The Indian Constitution acknowledges freedom of speech and expression as a constitutional right subject to reasonable restriction to uphold law and order, public health, morality, and decency, among other items. Sections 292 and 499 of the Indian Penal Code 1860, however, prohibit freedom of speech and language. It means that one cannot defame others while exercising their constitutional right to free speech and expression, and it bans expression through obscene content, as well as the publishing and dissemination of obscene material.

The facts of the case in *Maqbool Fida Husain vs Raj Kumar Pandey*[64] is that renowned painter MF Husain painted a nude lady in sorrow without giving it a title. In

[61] U.S. v. Joseph C. Bledsoe, 04-4276, 177 Fed. Appx. 311.
[62] U.S. v. Philip M. Sebolt, 04-2588, 460 F.3d 910
[63] U.S. v. Michael Shawn McCourt, 06-1018, 468 F.3d 1088.
[64]Maqbool Fida Husain v Raj Kumar Pandey, Delhi High Court Crl. Revision Petition No. 114/2007

2004, an untitled painting was sold to a private collector. Under the name 'Bharat Mata,' it was used in an online fundraising auction for victims of the Kashmir earthquake in 2006. Husain had no interest or role in this sale. There were massive demonstrations against the artwork, which was used in an auction commercial.Multiple cases were filed under the Indian Penal Code, 1860, sections 292, 294, and 298. The concern was whether the painting's representation of a naked woman as "Bharat Mata" should be deemed obscene under section 292 of the Indian Penal Code. "...the artistic touch to the artwork dwarfs the so-called obscenity in the form of nudity and makes it so picayune and trivial that the nudity in the painting can quickly be overlooked," the Court concluded. The naked woman was not portrayed in any odd poses, nor were her surroundings painted to evoke lewd feelings or desire.The Ashoka Chakra was also not put on any aspect of the woman's body that could be perceived as insulting to the national emblem.

"The literature of India, both religious and secular, is full of sexual allusions, sexual symbolism, and passages of such frank eroticism that are not found anywhere in world literature," the Court observed. "While an artist should have artistic independence, he is not free to do anything he wants," it added. The distinction that must be made is between art as an expression of beauty and art as an expression of an ill mind obsessed by a vulgar manifestation of counter-culture, the latter of which must be kept out of civilian society.""There should be freedom for the thinking we despise," the Court said. If there is no freedom after speech, freedom of speech is pointless. The degree to which democracy spreads equality and accommodation is a test of its reality."

Regarding film censorship, Chief Justice of the Supreme Court M. Hidayatullah held in *K.A. Abbas vs Union of India,*[65] that "our freedom of speech and expression is not absolute, but rather restricted by fair limitations under Article 19 (2) in the interest of upholding public decency and morality." As a result, in the area of cinematograph film, film censorship has total authority to prohibit and regulate obscenity and pornography."

While determining if the film "Satyam Shivam Sundaram" was obscene and indecent, the Supreme Court claimed in *Raj Kapoor and Others v State and Others,*[66] that

[65] K.A. Abbas v. Union of India, (1970) 2 SCC 780
[66] Raj Kapoor and Others vs State and Others, AIR 1980 SC 258

“While a certificate given by the Censor Board is appropriate, it does not prevent the court from deciding if a film is obscene or not.”

3.7 LET’S SUM UP

In this chapter, we have studied the meaning and definition of cyber and child pornography and how it is dealt with in the Information Technology Act, 2000, as well as the Indian Penal Code, 1860. Furthermore, we saw the different tests of obscenity observed by the Courts and ended the discussion with obscenity and freedom of speech and expression.

3.8 FURTHER READING

- Wolak J, Finkelhor D, Mitchell K. Internet-initiated sex crimes against minors: Implications for prevention based on findings from a National study. Journal of Adolescent Health 2004; 35:424.e11-424.e20.
- Quayle E, Taylor M. Child pornography and the internet perpetuating a cycle of abuse. Deviant Behavior 2002; 23(4): 331-361.
- Heck, Richard Kimberly (forthcoming). Pornography and Accommodation. _Inquiry: An Interdisciplinary Journal of Philosophy.
- Howitt D, Sheldon K. The role of cognitive distortions pedophilic offending: Internet and contact offenders compared. Psychology, Crime and Law 2007; 13(5):469-486.
- Ost S. Children at Risk: Legal and Societal Perceptions of the Potential Threat that the Possession of Child Pornography Poses to Society. Journal of Law and Society 2002; 29(3): 436-460.

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber pornography?**

Cyber Pornography can be defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials.

2. **In which case was the test of obscenity first described?**

In the case of *Regina vs Hicklin*, the test of obscenity was first described as the propensity “to deprave and corrupt those whose minds are open to certain forces and into whose hands a publication of this nature may fall,” with the assumption that this test will only extend to a isolated passage of the work.

3. **Explain Section 67 of IT Act?**

According to Section 67, obscene content in electronic form must be investigated individually to determine if it is so gross and its obscenity so defined that it is likely to deprave and degrade those whose minds are vulnerable to such effects and into whose hands the obscene material in electronic form is likely to fall.

3.10 ACTIVITY

Elucidate the test of obscenity and pornography and which test is currently adopted by the Indian Courts and why? (1500-2000 words)

Unit 4: CYBER WARFARE

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Information as a Tool of War

4.4 Objectives of Cyber Warfare

4.5 Types of Cyber Warfare Attacks

4.6 Examples of Cyber Warfare

4.7 Indicators of Cyber Warfare Capabilities

4.8 The Government Sector

4.9 The Private Sector

4.10 Cyberwarfare and Role of India

4.11 Let's sum up

4.12 Further reading

4.13 Check your progress: Possible answers

4.14 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- How information is being used as a tool of war
- Indicators of cyberwarfare capabilities
- Cyberwarfare and role of India

4.2 INTRODUCTION

The cyber warfare world was created by combining several elements from the experience of human conflict. Certain forerunners developed dispute standards that now extend to the cyber domain well before the advent of the machine and the ability to communicate on the Internet. This chapter looks at the role of intelligence in the history of human war, including both the effort to learn about the adversary and the desire to keep the information safe from enemies. The relentless search for fresh and reliable knowledge has affected every area of conflict across computer networks as cyber operations have become more widespread.

Cyberwarfare is computer or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyberespionage.

Although cyber warfare generally refers to cyber attacks perpetrated by one nation-state on another, it can also describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. It can be difficult to definitively attribute cyber attacks to a nation-state when those attacks are carried out by advanced persistent threat (APT) actors, but such attacks can often be linked to specific nations. While there are a number of examples of suspect cyber warfare attacks in recent history, there has been no formal, agreed-upon definition for a cyber "act of war," which experts generally agree would be a cyber attack that directly leads to loss of life.

Cyber warfare can take many forms, including:

- viruses, computer worms and malware that can take down water supplies, transportation systems, power grids, critical infrastructure and military systems;
- denial-of-service (DoS) attacks, cyber security events that occur when attackers take action that prevents legitimate users from accessing targeted computer systems, devices or other network resources;
- hacking and theft of critical data from institutions, governments and businesses; and
- ransomeware that holds computer systems hostage until the victims pay ransom.[67]

4.3 OBJECTIVES OF CYBER WARFARE

According to Cyber security and Infrastructure Security Agency (CISA), the goal of those engaged in cyber warfare is to "weaken, disrupt or destroy the US." To achieve their goals, "national cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests," says CISA. These threats range from propaganda to espionage and serious disruption with loss of life and extensive infrastructure disruption. A few examples of threats include:

- Espionage for technology advancement. For example, the National Counterintelligence and Security Center (NCSC) in its 2018 Foreign Economic Espionage in Cyberspace report notes that China's cyber security law mandates that foreign companies submit their technology to the Chinese government for review and that Russia has increased its demand of source code reviews to approve of foreign technology sold in their country. In 2018, the US Department of Justice charged two Chinese hackers associated with the Ministry of State Security with targeting intellectual property and confidential business information.
- Disruption of infrastructure to attack the US economy or, when attacked by the US, to damage the ability of the US to continue its attacks. For example, by controlling a router between supervisory control and data acquisition (SCADA)

[67]https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

sensors and controllers in a critical infrastructure, such as the energy sector, an enemy can attempt to destroy or badly damage energy plants or the grid itself.

Cyber attacks are also used to sow discord to destabilize government. For example, according to Report On The Investigation Into Russian Interference In The 2016 Presidential Election, by Special Counsel Robert S. Mueller, III, Russia's Internet Research Agency "used social media accounts and interest groups to sow discord in the U.S. political system through what it termed 'information warfare.' The campaign evolved from a generalized program designed in 2014 and 2015 to undermine the U.S. electoral system, to a targeted operation that by early 2016 favoured candidate Trump and disparaged candidate Clinton."[68]

4.4 TYPES OF CYBER WARFARE ATTACKS

Increasingly, cybercriminals are attacking governments through their critical infrastructure, including transportation systems, banking systems, power grids, water supplies, dams, hospitals and critical manufacturing.

The threat of cyberwarfare attacks grows as a nation's critical systems are increasingly connected to the internet. Even if these systems can be properly secured, they can still be hacked by perpetrators recruited by nation-states to find weaknesses and exploit them.

APT attacks on infrastructure can devastate a country. For example, attacks on a nation's utility systems can wreak havoc by causing widespread power outages, but an attacker with access to hydropower grids could also conceivably cause flooding by opening dams.

Cyberattacks on a government's computer systems can be used to support conventional warfare efforts. Such attacks can prevent government officials from communicating with one another; enable attackers to steal secret communications; or release employee and citizen personal data, such as Social Security numbers and tax information, to the public.

[68]https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

Nation-state-sponsored or military-sponsored attackers might also hack the military databases of their enemies to get information on troop locations, as well as what kind of weapons and equipment they're using.

DoS attacks, which continue to increase around the world, are expected to be leveraged for waging cyberwarfare. Attackers are using distributed denial of service (DDoS) attack methods to hit government entities with massive sustained bandwidth attacks, and at the same time infecting them with spyware and malware to steal or destroy data. These attacks may inject misinformation into the networks of their targets to create chaos, outages or scandals.[69]

4.5 EXAMPLES OF CYBER WARFARE

Perhaps the earliest instance of a nation waging cyberwar was the Stuxnet worm, which was used to attack Iran's nuclear program in 2010. The malware targeted SCADA (supervisory control and data acquisition) systems, and was spread with infected USB devices; while the United States and Israel have both been linked to the development of Stuxnet, neither nation has formally acknowledged its role.

Nation-state actors are believed to be behind many other cyberwarfare incidents. For example, in March 2014, the Russian government allegedly perpetrated a distributed denial-of-service attack that disrupted the internet in Ukraine, enabling pro-Russian rebels to take control of Crimea.

Then in May 2014, three days before Ukraine's presidential election, a hacking group based in Russia took down Ukraine's election commission's system, including the country's backup system. However, Ukrainian computer experts were able to get the system up and running before the election. The cyberattack was launched to wreak havoc and damage the nationalist candidate while helping the pro-Russian candidate, who ultimately lost the election.

[69] https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

Hackers associated with the government of North Korea were blamed for the 2014 cyberattack on Sony Pictures after Sony released the film The Interview, which portrayed the North Korean leader Kim Jong-un in a negative light.

During its investigation into the hack, the FBI noted that the code, encryption algorithms, data deletion methods and compromised networks were similar to malware previously used by North Korean hackers. In addition, the hackers used several IP addresses associated with North Korea.

A 2015 attack on the German parliament, suspected to have been carried out by Russian secret services, caused massive disruption when the attack infected 20,000 computers used by German politicians, support staff members and civil servants. Sensitive data was stolen, and the attackers demanded several million euros to clean up the damage.

Although a group of Russian nationalists who wanted the government of Berlin to stop supporting Ukraine claimed responsibility, members of the Russian intelligence were also reported to be involved.

Since then, a Malware Analysis Report (MAR) issued by the Department of Homeland Security (DHS) and the FBI identified two malware codes, HOPLIGHT and ELECTRICFISH, released by North Korea.

Also in 2015, cybercriminals backed by the Chinese state were accused of breaching the website of the U.S. Office of Personnel Management to steal data on approximately 22 million current and former employees of the U.S. government. Chinese cybercriminals have been implicated in the theft of U.S. military aircraft designs, an incident that caused then-president Barack Obama to call for a treaty on cyberarms control.

On a cold winter's day in December 2016, more than 230,000 customers in Ukraine experienced a blackout, the result of remote intrusions at three regional electric power distribution companies. The attack was suspected to originate from Russia. The perpetrators flooded phone lines with a DoS attack and also used malware to attack and destroy data on hard drives at the affected companies. While the power

was restored within hours, it took months for the companies to restore full functionality to the control centers that had been attacked.

In 2016, 2017 and again in 2018, variations of malware known as Shamoon struck businesses in the Middle East and Europe. McAfee's Advanced Threat Research concluded that the Iranian hacker group APT33, or a group masquerading as APT33, is likely responsible for these attacks.

On August 2, 2017, President Trump signed into law the Countering America's Adversaries Through Sanctions Act (Public Law 115-44) (CAATSA), imposing new sanctions on Iran, Russia, and North Korea.70

4.6 INFORMATION AS A TOOL OF WAR

Knowledge operations have been used to gain benefits in combat for as long as humans have participated in something that could be defined as "warfare." Attempts to observe enemy troop dispositions or diversion activities to conceal one's own troops in an ambush situation were examples of traditional intelligence campaigns. For gathering intelligence on the enemy's resources and intentions, an effective military leader can depend on a vast network of spies. This kind of spying may be carried out by uniformed scouts or by a camouflaged insider posing as a loyal member of the enemy's military.Of course, information was only valuable if it could be correctly shared in a timely manner, and information delivery posed inherent risks. If an adversary intercepts a messenger, the letter is lost, and the intelligence is sent to the opposing officer. As a result, it could be appropriate to send the message only verbally, in the hopes that the messenger may not leak the information, or in an encrypted script that the enemy may not be able to decipher.Fake communications may be intentionally leaked to the enemy to obstruct decision-making and fog the intelligence available to an adversary.

Since cyber warfare is such a novel phenomenon, it raises much more questions than it answers. The importance of cyber assets in national defence, the feasibility of a cyber policy, and even if the word "warfare" should be used to describe cyber operations are all topics that spark heated discussion. Many cyber operations, such

[70]https://searchsecurity.techtarget.com/definition/cyberwarfare#:~:text=Cyberwarfare%20is%20computer%2D%20or%20network,or%20military%20purposes%20and%20cyberespionage.

as fraud, espionage, and terrorism, have elements of warfare but do not fall within conventional categories.

4.7 INDICATORS OF CYBER WARFARE CAPABILITIES

Because of the technology's existence, the ability to produce and employ nuclear power, whether for peaceful or destructive purposes, was limited to a few developing nations when it was first developed. If a country decided to go nuclear, not only was the equipment difficult to obtain but the selected few powers still assured that ample obstacles were placed in their way. Then there was the threat of nuclear proliferation, which prohibited countries from using nuclear weapons in combat.As a result, the number of countries with nuclear weapons systems remained low. Some countries, such as North Korea and Iran, were quickly identified as attempting to develop a nuclear weapon covertly since there were few countries capable of acquiring the equipment for such a weapon system, and there was also a ban on the transfer of such technologies. Many of these aspects together meant that nuclear power remained a bastion of a chosen few.

This is not the case, though, for cyber technology.Information technology is unlike any other weapon system technology because of its inherent design and accessibility. It's perhaps the first commercial technology that can also be used for military purposes. As a result, the factors determining a nation's ability to fight a cyberwar would vary from those determining traditional or nuclear strength. Although determining a nation's nuclear and conventional warfighting capability is easy, determining a nation's cyber might is more complex.As a result, it's critical to figure out what considerations all go into cyberwar waging capability.

The government sector and the private sector are the two broad types of sources that are indicators of a nation's electronic warfare capability.

4.8 THE GOVERNMENT SECTOR

- ***Available Cyber Warfare Doctrine***

If a nation declares a cyber warfare policy, it is clear that the country has superior cyber capabilities. There is no time to think of a systematic solution during a

cyberattack.A Cyber Warfare Doctrine outlines the roles of all players in the event of a cyberattack, provides a clear picture of the national response in the event of such an attack, and helps to prevent possible conflicts by a unified national security strategy. Just a few countries have issued an electronic warfare policy to date.

- ***Active Cyber Warfare Units***

If a nation wants to conduct offensive cyber operations while still protecting its own infrastructure, especially military infrastructure, it must be well prepared. As a result, those countries' military forces will have organizations capable of electronic warfare. A successful cyberwarfare organization will range from a national cyber command to a small unit capable of conducting cyberattacks. Several countries have either raised or are in the process of raising those powers. On the other hand, several countries have clandestine units capable of conducting cyber operations.In May 2013, India's former Defence Minister, Shri AK Antony, announced that the country would soon form a cyber command to deal with the country's online attacks.[71]About the fact that the cyber command is yet to see the light of day, the armed forces remain optimistic that the current government will eventually allot the funds needed to upgrade this strategic asset in India.

- ***Computer Emergency Response Teams (CERT)***

The Computer Emergency Response Team (CERT) is a government-mandated information technology security organization. The mission of the Computer Emergency Response Team (CERT) is to respond to computer security events, report vulnerabilities, and encourage successful IT security practices around the nation. CERT may exist at different levels, ranging from the national level to the level of a single organization. CERTs are now used by a variety of military forces around the world.

- ***Cyber Crime Prevention / Investigation Teams***

Although the aim of such teams is to combat and prosecute cybercrime, the essence of their work allows them to be an important weapon for defensive cyber operations.

- ***Government-run Academic Institutions with Cyber Programs***

Such organizations explicitly demonstrate that the government intends to build a skilled pool of manpower that can be used to conduct both defensive and offensive

[71] Cyber Command for Country Soon: Antony TNN May 26, 2013, 03.09AM IST

cyber operations. Ethical hacking programmes are conducted in a variety of countries, including India, to educate white hat professionals.

- ***Government Sponsored Cyber Projects***

A significant number of countries fund defence-related information infrastructure programmes, such as cyber-training programs. The aim of such programs may be to conduct research and development in the area of cyber technology, which can then be effectively used in strategic and tactical cyber warfare operations. Under the guise of R&D, some countries need such programs to conduct cyber espionage and surveillance.

- ***Intelligence Service Capabilities***

Intelligence is a critical component of cyber operations. When a country's government or security forces invest in cyber intelligence, it's safe to say that the country is indeed investing in cyber warfare capability.

- ***Military Command and Control Communications, Computer and Intelligence (C4I) and Information Warfare Capability***

To be a force multiplier, cyber-warfare must be integrated into a country's overall combat policy. As a result, cyber activities must be blended into the military's overall information warfare and C4ISR policy. If a country's military forces, such as the United States', have well-developed C4ISR capabilities, they will be able to conduct cyber operations with much greater ease than a country with little or limited C4ISR assets.

- ***Military Intelligence Units***

When a nation is attempting to develop aggressive cyber warfare capability, military intelligence teams are almost always tasked with gathering knowledge about the enemy's operating networks and IT processes. It will be difficult to carry out any cyberattacks during a war without this vital piece of intelligence.

- ***Military Units Capabilities***

Military technologies are being updated all over the world to track the rapidly evolving cyberspace, conduct cyberattacks, and protect against them. Armed forces are being trained and prepared to counter the vulnerabilities of the enemy's cyber warfare.The development of such technologies is the most telling sign that a country is attempting to acquire offensive cyber warfare capabilities.

- ***Overall use of IT***

The very presence of networks in a nation's security forces, as well as its reliance on information technology for day-to-day operations, indicates that the country is prepared for cyber warfare. A well-connected army, navy, or air force would undoubtedly invest in cyber defence. If a force has defensive cyber warfare capability, it is almost assured that it will also have aggressive cyber warfare capabilities.

4.9 THE PRIVATE SECTOR

Although strong-armed forces are needed for a nation to fight a war, this is not the case for cyberwar. Non-state actors, cyber terrorists, and even state-sponsored hackers will engage in aggressive cyberwar/ cyber operations, unlike other means of warfare.A country's private IT technology is sufficient to ensure that the country is prepared for cyberwar. As a result, the state of growth of the private sector is just as critical as a measure of a country's cyber warfare capacity. The following are some of the aspects:

- ***Academia***

A well-developed educational infrastructure in computer science and engineering enables the country's youth to be prepared for a variety of IT-related activities.The same youth can be used to create a solid electronic warfare foundation.

- ***Accessibility of network to the general public***

The greater the infiltration of facilities such as the internet, the more likely the nation would have cyber warfare capability.

- ***Computer security programs***

The nation's cyber defence would be stronger than most as it is capable of designing or even enforcing sound information security systems.

- ***Expatriate students studying in technologically advanced countries***

China serves as an excellent example of this. According to the Minnesota Daily, between 2009 and 2012, US universities enrolled approximately 100,000 Chinese students, accounting for roughly a quarter of all international students in the country.[72] China now has one of the strongest offensive cyber capabilities.

[72] Department of Homeland Security, Study in the States as available at

- ***Fiber optic cable/copper wiring***

The physical network's size means that voice and data networks can cover even the most distant parts of the world. The wider the scope, the greater the number of users who have access to the internet.

- ***Hackers***

Hackers may be state-sponsored, sanctioned black hats and cybercriminals with clear political objectives. To educate security professionals, several countries run ethical hacking colleges.The more schools there are, the greater the pool of hackers open to the nation.

- ***Hardware production capabilities***

The country's overall development in the field of IT is reflected in its hardware development capability.

- Other considerations may include:
    a) public access to high-speed internet
    b) private sector IT collaboration with other countries
    c) IT networks in the world
    d) presence of IT defence firms in the country
    e) number of ISPs and key nodes
    f) The number of satellite connections that have nationwide network access
    g) Telephone line density
    h) Overall state and IT incorporation
    i) SCADA (supervisory management and data acquisition) systems are examples of process control systems
    j) Skills in software growth
    k) Transnational companies with an interest in or use of information technology

The above metrics indicate that the more mature a country's private IT and telecom industries are, the more likely it is that the country will be able to engage in cyber warfare. In either event, countries with well-developed telecom and IT industries, such as Japan, Taiwan, and India, would need to brace for cyberattacks by rogue

---

http:// studyinthestates.dhs.gov/2014/01/number-of-chinese-students-studying-inthe-united-states-increases

nations and rogue elements. This ensures that defensive cyber capability becomes an inextricable aspect of a country's well-developed IT and telecom industries.

4.10 CYBER WARFARE AND ROLE OF INDIA

Cyberwarfare does not merely involve some countries as perpetrators and some as victims. Cyberwarfare is involved in all social spheres, it is all around us, and we encounter it every day. Every individual has used a fighting technique to gain information at least once in their lives, but this was not necessarily illegal and was mostly of no significance. In the context of cyberwarfare at the national level, among organizations, or by ideological, media and major interest groups, the warfare techniques and their consequences are often socially harmful. The struggle for information includes all countries and their entities. However, some are more aggressive than others because they devote more resources to the development of this field.

Different countries, in terms of their size, economic performance and political orientation, understand the importance and benefits of cyberwarfare and develop its techniques. In fact, it is not clear which entities are more successful in achieving this. The involvement of ICT in government and organizational structures is not necessarily an advantage since it can also represent a weakness in terms of risk. Countries mentioned as the main cyberwarriors (the United States, China and Russia) can be gradually equated with countries that are less dependent on ICT, closed and inaccessible (e.g. North Korea). The United States is certainly the world's leading political, economic and military superpower, which makes it the most popular target for malicious intrusions and attacks on information systems.

In the field of software development, India is an extremely powerful country, but we know little about its activities in cyberwarfare.[73] After the cyberattack India experiences in the summer of 2012, in which officials from the Ministry of External Affairs, the Ministry of Home Affairs, the Defence Research and Development Organization (DRDO), and the Indi-Tibetan Border Police)ITBP) were attacked, and a lot of sensitive information was under threat, it was found that approximately 12,000 computers were affected. At that time, the responsibility for preventing attacks was assigned to the Indian Computer Emergency Response Team (CERT-In), which is a branch of the Department of Information Technology. CERT-In

[73] Taken from Dala [DAL 11], Tiwary [TIW 11] and Kaushik and Fitter [KAU 13].

announced that the number of *'cybersecurity breaches has grown from 23 in 2004 to 13,301 in 2011'*. Because of these breaches, the government divided the CERT-In, in order to better prepare the country for serious threats: *'CERT-In now protects cyber assets in non-critical areas while a new body called the National Critical Information Infrastructure Protection Centre (NCIIPC) protects assets in sensitive sectors such as energy, transport, banking, telecom, defence, and space'.*

The government notes that more attention must be invested in research and development, whereas NCIIPC is preparing the final version of the national cybersecurity policy. In general, India has not suffered any major economic or physical harm due to cyberattacks. However, the government-owned Nuclear Power Corporation of India is at constant risk of security breach, since it continuously detects attacks but is, in its opinion, able to successfully block them. India admits that its cyberwarfare defence strategy was tackled too late and, consequently, it detects attacks on their infrastructure, but is now increasingly preparing adequate strategies and focusing its expertise on the development of this field so that in future India will be able to defend itself from attacks and join other countries that are active in the field of cyberwarfare.

4.11 LET'S SUM UP

In this chapter, we have studied how information can/is being used as a tool of war along with the indicators of cyberwarfare capabilities. Furthermore, we saw the government and private sector indicators and ended the discussion with the role of India in cyberwarfare.

4.12 FURTHER READING

- Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners by Jason Andress and Steve Winterfeld 7. Surviving Cyberwar by Richard Stienno
- Guidelines for Protection of National Critical Information Infrastructure, Version 1.0 (June 2013), issued by National Critical Information Infrastructure Protection Centre 14. Indian Army Doctrine, First edition, October 2004
- Cyber Deterrence and Cyberwar, Rand Corporation monograph by Martin C. Libicki 16. UN Convention on Cybercrime, CETS No.: 185

- Revamping India's National Security Architecture for Optimum Synergy in the Use of its Instruments of National Power, The 18th Pyara Lal Memorial Lecture, 2014 by Shri Shyam Saran, IFS (Retd) 21. National Cyber Security Framework Manual, Edited by Alexander Klimburg

4.13 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is CERT?**

The Computer Emergency Response Team (CERT) is a government-mandated information technology security organization. The mission of the Computer Emergency Response Team (CERT) is to respond to computer security events, report vulnerabilities, and encourage successful IT security practices around the nation.

2. **Name 3 indicators in private sector?**

- Computer security programs
- Hackers
- Hardware production capabilities

3. **What is C4ISR policy?**

To be a force multiplier, cyber-warfare must be integrated into a country's overall combat policy. As a result, cyber activities must be blended into the military's overall information warfare and C4ISR policy. If a country's military forces, such as the United States', have well-developed C4ISR capabilities, they will be able to conduct cyber operations with much greater ease than a country with little or limited C4ISR assets.

4.14 ACTIVITY

Elucidate the Government and Private sector as indicators of cyberwarfare along with a few case studies. (2000-2500 words)

What is cyber warfare? What are its types? Explain cyber warfare with suitable examples. (2000-2500 words)

Block-4

INTERNATIONAL LAW ON CYBER SPACE

Unit 1: INTERNATIONAL LAW ON CYBER SECURITY IN THE AGE OF DIGITAL SOVEREIGNTY

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Existing challenges on international law and governance on cyberspace.

1.4 Digital Sovereignty in India

1.5 International law on cyber space and digital sovereignty

1.6 Concluding remark

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible Answers

1.10 Activity

1.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Existing challenges on international law and governance on cyberspace, and
- International law on cyberspace and digital sovereignty.

1.2 INTRODUCTION

Recent trends in the promotion of digital sovereignty have increasingly deprived us of the complexity and challenges of international law in cyberspace. Digital sovereignty is the ability to control and direct international actors through the use of digital technologies such as the Internet, social media, and other digital media. Although international law is still at an early stage, there is an urgent need for how it is applied in this area, but this is a long game

and is still in its infancy. This article is divided into two parts: a brief overview of the existing challenges for international cyber law and a discussion on the impact of these challenges on the future of cybersecurity.

Thomas Aquinas in his magnum opus Summa Theologica mentioned,“law is an ordinance of reason for the common good, made by those who have care of the community” (Aquinas, 1981). Unfortunately, this adage does not necessarily resonate to international law on cyberspace. The absence of effective international legal instruments on cyberspace has largely been discussed in theoretical and policy-making debates as the complexities in cyberspace render difficult for actors to come into agreements, let alone making agreeable binding law. The contentious academic debates chiefly divide those who believe that states must take more influential roles in formulating international law on cyberspace and those who insist that cyberspace should remain a free and diffused domain. Beyond academic textbooks, more dynamic debates take place by stakeholders and in international institutions (World Economic Forum, 2019; Opinio Juris, 2019). All of these debates reach into one converging point: the absence of international legal regime on cyberspace is derived from actor’s complexity and jurisdiction on cyber realm. This is further complicated by the fact that in the past few years several international actors, mostly state actors, promote the idea of digital sovereignty to promote their

interest to take back control on information, communication, data, and infrastructure related to the internet (Gueham, 2017). Consequently, this creates harder challenges on possible future international law on cybersecurity. The future of international law on cyberspace would also hardly apply to states' conduct due to the increasing trend of promotion of digital sovereignty norms.

> Sovereignty is one of the non-negotiable policies for ensuring the security of the country. Sovereignty ensures that we as a nation can stand up to pressures from other countries. Sovereignty is critical to ensure our economic independence.
>
> As Information Technology is playing an increasingly important role in India's economy, it becomes imperative to identify the issues of Digital Sovereignty and to formulate appropriate policies to ensure our Digital Sovereignty.
>
> So why is it that India's Digital Sovereignty is threatened? The threat to India's Digital Sovereignty is primarily coming from two areas i.e., the digital standards and the control of the Internet.
>
> Digital Standards are being used extensively to extract undue economic benefit from emerging economies such as India wherein a corporate or a coterie of corporates, typically based in the West, creates a standard and files numerous IPR encumbrances such as patents around the standard. The standard is then taken through one or more international standardization bodies and is turned into an international standard which is then forced unto the users in emerging economies. The users of the standard are then forced to pay disproportionate royalties either directly, or indirectly by paying a higher price for the end products with the manufacturers having to cough up the unfair royalties. The nation-state is helpless in this situation as any intervention will be either a TBT violation (Technical Barrier to Trade) or will be a violation under TRIPS.
>
> A very good example of the devastating effect that such a lack of Digital Sovereignty can have is the case of the DVD manufacturers in China. The DVD manufacturers have to pay royalty charges on each DVD player manufactured in China that is to the tune of 33% of the retail price of the DVD player, for a video format standard that is used as a standard in each DVD

player. This works out to be $20 royalty on a player of $60. As a response, China came out with an alternative video encoding standard called AVS (audio-video standard) so that its manufacturers could use this standard without any undue royalties. However, because of the global technology framework that has evolved, AVS could not significantly help alleviate the situation of the DVD manufacturers in China. China was helpless in preventing such an unfair cess being put on its domestic industry, demonstrating its lack of Digital Sovereignty then.[74]

1.3 DIGITAL SOVEREIGNTY IN INDIA

As India gets more and more dependent on its IT economy, we are going to see more similar issues coming up. The best example of such a situation was the recent case of Microsoft forcing its standards into ISO even though India and a majority of the population of the world voted against it. India again lost its digital sovereignty in this case on a technology that is critical for ensuring digital literacy in the country.

However, India as a nation has only recently woken up to the threat to the nation due to India's lack of control over IT standards and control over the Internet. The Indian government has only in the last half a decade, initiated steps to protect its citizens and businesses from foreign entities imposing their standards on India and Indians. Foreign entities are extracting royalties from the Indian economy without any significant contribution back to the economy.

On the other hand, after China was forced to back down on its aggressive stance on coming out with an alternate wireless LAN standard called WAPI (with the then US Vice President Dick Cheney personally leading the pressure on China), China put together a comprehensive technology standards strategy to protect its Digital Sovereignty.

The second issue which is threatening India's Digital Sovereignty is its ability to protect its interest in the Internet.

[74] https://www.outlookindia.com/website/story/opinion-standards-and-internet-the-cornerstones-for-digital-sovereignty/376498

The visceral of the Internet is primarily controlled by ICANN that determines the allocation of website addresses and machine addresses (IP addresses) through which computers and websites can be identified and accessed. ICANN is a California based company under US legal jurisdiction and it does not come under the jurisdiction of Indian law. Every individual/ business/ government that wants to set up a website on the Internet, has to pay directly or indirectly to ICANN to get the website name and/or the IP address. The lack of our digital sovereignty has ensured that we have very little formal control over how the Internet is governed and that we and our people have to pay unjust amounts to a US company. Also, ICANN has come out with more Top Level Domains (TLD's). What this means is that ICANN can issue a name and we will have no control over it. Or it can come out with unacceptable sites with names of Gods and Goddesses at the end of the name with the Government of India having no control over it while riots break out in India. Of course, ICANN has now moved to a governance format which is termed as “multistakeholderism”.

Loss of Digital Sovereignty makes our IT industry vulnerable and ephemeral as the real control over technology continues to stay with developed economies.

It is the need of the hour for India to come out with a robust Digital Sovereignty policy that protects our IT industry and our consumption of Information Technology. In the absence of such a policy, we stand to get arm-twisted and our businesses will have to give out undue payoffs to non-Indian agencies for using technologies that are fundamental to our economy. It also includes having control over what goes into the building of our IT infrastructure, telecom switches and set-top boxes.[75]

1.4 EXISTING CHALLENGES ON INTERNATIONAL LAW AND GOVERNANCE ON CYBERSPACE

The idea of regulating cyberspace by international law is not something remarkably novel. Since 1996, the efforts of formulating international law on cyberspace have already been continuously proposed (and refuted) by law experts, business actors, and states. There are three dominant ideas on how cyberspace should be regulated by international law: Liberal Institutionalists, Cyberlibertarian, and Statists. Liberal institutionalists like Wu (1997) call for the importance of the

[75] *Ibid.*

international institution and rule-based multilateralism in managing cyberspace. While cyberlibertarians like John Barlow (1996) are proponents of the idea that cyberspace should remain free from tyranny and any oppressive rule that might hinder the internet liberty . Statists, like James Lewis (2010), believe that it is states' responsibility to formulate national and international law to govern cyberspace. These three mainstream ideas echo into the development of international law on cyberspace. Binding and well-functioning international law on cyberspace is still absent due to these ongoing contentious debates. These debates rest on to three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

Jurisdictions in international law according to Basak Cali (2015) relates largely to the subject of international law (or actors in international relations) and territoriality to which law may be formally exercised. The subject of law or actors in cyberspace are widely diverse and diffused as it ranges from state actors, big internet companies, small-medium enterprises (SMEs), hackers, to individuals–not to mention that internet innately also provides anonymity to its users. Those various actors also bear their own different interests and issues on how cyberspace should be regulated. It is still immensely challenging to address which subjects of law are legitimate to make and be affected by international law on cyberspace, as well as what issues should be regulated. This is also increasingly challenging to attribute conducts made by actors and where it is conducted.

Numerous debates either in academic texts or policymaking have been rendered specifically discussing attribution on cyber conduct (Rid & Buchanan, 2014). Yet, there is no single dominant and prevailing voice in that debate except for those attribution of cybercrime from state actors to nonstate actors in which it is relatively agreed and functioning in international regimes, such as exemplified in Interpol, Europol, ASEANAPOL, and UNODC. In terms of domain in cyberspace, international actors have not come into agreement on the status of cyberspace whether it is global commons, belongs to physical states' territory, or based on their national origins (Liaropoulos, 2017). As a result, it creates major challenges to determine jurisdiction of international cyber law until today.

The complexity of actors and issues discussed above render further complications in arbitration. Public international law necessitates clear dispute settlement mechanisms and arbitration to ensure that law is enacted and binding its signatories and subjects (Cali, 2015). In cyberspace law, due to its actors' diversity, there is still no universally agreed legal norm reached on who should get the mandate of dispute settlement mechanisms and arbitration. There is already arbitration on cyberspace conducts but mostly it is related to commerce and crime in which it takes place in the national legal system rather than international court (Kittichaisaree, 2017). Thus, this potentially undermines the impartiality of law since states presumably have greater bargaining power in such a legal system. Nevertheless, it is not impossible to have possible international arbitration in cyberspace. Permanent Court of Arbitration in The Hague, Netherlands might have the potential to be addressed as adjudication party on cyberspace as it already has a mandate on outer space, energy, and environmental cases. However, it needs major approval from state actors to push such mandates and authorities on cyberspace cases.

Related to arbitration, one must take into account the cyberspace challenges of legal instruments and jurisprudence. Both take place in two levels: national and international. Legal frameworks addressing cyberspace are relatively already well-developed in developed countries. In the federal level, U.S. has three fundamental regulations enacted in HIPAA (1996), Gramm-Leach-Billey Act (1999), and Homeland Security Act (2002). In France, the national authority has enacted and developed legal frameworks on cyberspace since 1988. In Russia, the federal authority also adopted the Russian Federal Law on Personal Data no. 152 FZ since 2006 (Kittichaisaree, 2017). However, those countries take a different standpoint on cyber space as Russia controversially stipulates security concern as a priority over privacy rights and the U.S. have a similar problem since Snowden's issue rise into public attention. This disparity will be widened out if we delve into cyber legal frameworks in developing countries such as Malaysia and Indonesia. Malaysia does not have a standalone cyber act or bill in which it creates room for deep state' intervention to citizen's data (ICLG, 2019).

Indonesia is in worse condition–its proposed law on cybersecurity was postponed to be adopted due to massive student demonstrations in the last few months

caused by human rights concerns (Jakarta Globe, 2019). These national legal framework disparities show how the absence of effective international law on cyberspace stems from national legal instruments. On the international level, the law on cybersecurity is scarce. Indeed there is Budapest Convention which is claimed to be the only international treaty on cyberspace. But one must not deny the fact that this is a lack of binding dispute settlement mechanism, tends to be state-centered, and focus profoundly on cybercrime. There is also a series of discussions on encouraging international customary law to be the foundation of international law on cyberspace (Brown & Poellet, 2012). Yet, international customary law requires reified practice and solidified legal instruments performed at the national level. As mentioned above, this is still improbable due to disparities of the national legal system on cyberspace in various countries. Efforts to formulate regulation also occur in various institutions, such as ITU, ICANN, and Internet Governance Forum in regard to governing fundamental norms, principles, and operationalities of cyberspace (Deibert & Crete-Nishihata, 2012). Unfortunately, none of those manages to overcome how international law applies effectively to states and addresses various issues in cyberspace beyond cybercrime and technicalities. None of those successfully creates appropriate and binding international legal instruments and jurisprudence. Ergo, international law on cyberspace currently is hardly effective and more difficult to be imposed on state actors.

1.5 INTERNATIONAL LAW ON CYBER SPACE AND DIGITAL SOVEREIGNTY

The complexities and challenges of international law on cyberspace are increasingly deprived by a recent trend on digital sovereignty promotions. Digital sovereignty is the idea to control and govern access, information, communication, network, and infrastructure in digital realm by international actors (Couture & Toupin, 2019). In recent years, this idea has been gaining traction because of three historical conjunctures in cyberspace: China and Russia cyber alliance on digital sovereignty; Snowden and Wikileaks cases; and the rise of GAFA (Google-AppleFacebook-Amazon). China and Russia cyber alliance on digital sovereignty becomes the major precursor of digital sovereignty as both countries actively

promote such an idea in order to protect their national interests which mostly are related to economy and security concerns. Both countries demand greater control of their own cyberspace by underpinning the principle of non-interference in multiple global internet governance such as ITU, ICANN, IANA, and Internet Governance Forum (Budnitsky & Jia, 2018). This sparks debate on whether the idea of digital sovereignty is against internet neutrality or not (Mueller, 2012).

However, their efforts influentially shift the paradigm of state control over their cyberspace as that idea is supported by countries like Saudi Arabia and Egypt (Deibert & Crete-Nishihata, 2012). Their efforts also invoked the European Union to reconsider letting internet in laissez-faire mode continue as Snowden-Wikileaks cases rose into public attention. Security and data protection concerns have increasingly become the center of debate gravity on whether the European Union should support (Dworkin, 2015). Later, this concern has broadened up to economic consideration due to the unchecked behavior of rising big internet companies, especially GAFA. The astronomical rise of GAFA made EU consider their digital ecosystem in order to prevent business monopoly and support the innovation and internet capabilities throughout Europe (Stormshield, 2018).

These situations unequivocally set new climate of international law on cyber space in favorable to state actors. These digital sovereignty promotions and advancements would not only potentially undermine particularly non state actors and internet neutrality as the questions of freedom and liberty in cyberspace consequently emerge. These also erode the potential agreeable international law on cyber security. It is because digital sovereignty would potentially create the fragmented cyber space as it will be regulated profoundly by states on territorial basis. The idea of digital sovereignty would disconnect global internet as it is now. As a result, it hardens the possibility of international actors to come into agreement to formulate effective and binding international law on cyber space. It also hardens the possibility to adjudicate cases of cyber violations to state actors since digital sovereignty is engrained with noninterference principles–it is difficult to punish and blame state actors for their conduct in arbitration as we have seen in International Criminal Court. Alternatively, if this idea of digital sovereignty would converge state actors to come into agreement to formulate international cyber law, the law itself would be presumably dominated and determined by state actors interests with their

contesting ideas of digital sovereignty at the expense of non-state actors such as business companies, individual citizens, and civil societies.

1.6 CONCLUDING REMARK

The question of does international law apply to states' conduct on cyber space as discussed above denotes that the answer is not effectively. It is derived from the past and current challenges on three aspects of international law: jurisdiction, arbitration, and legal instruments & jurisprudence. In the future, the trend on increasingly promoted digital sovereignty norms potentially drive future international law on cyber space to be hardly effectively imposed on state actors. If, any, the future international law on cyber space would be nuanced by digital sovereignty at the expense of their non-state actors interests. Both scenarios show that international law on cyber space is hardly effective for state actors and need broader calls for formulating rule-based, freedom-based, and inclusive global internet norms in the future.

1.7 LET'S SUM UP

In this chapter, we understood the binding and well-adjudicated international law on cyberspace, which does not effectively apply to states given challenges taken place in public international law related to jurisdiction, arbitration, and legal instruments & jurisprudences.

1.8 FURTHER READING

- Dworkin, Anthony. 2015. "Surveillance, Privacy, and Security: Europe's Confused Response to Snowden",ECFR Policy Memo. Franklin, M.I. 2010.
- "Digital Dilemmas: Transnational Politics in the Twenty-First Century",The Brown Journal of World Affairs, 16(2): 67-85. Gueham, Farid. 2017.
- Digital Sovereignty – Steps Towards a New System of Internet Governance. Paris: Fondapol. Jakarta Globe. 2019.
- Cybersecurity Bill Postponed Until Houses Next Term. https://jakartaglobe.id/context/cybersecurity-bill-postponed-until-houses-next-term/ ICLG. 2019.

- Cybersecurity Laws and Regulations: Malaysia. https://iclg.com/practice-areas/cybersecurity-laws-andregulations/malaysia Kittichaisaree, Kriangsak. 2017.
- Public International Law of Cyberspace. New York: Springer. Lewis, James A. 2010.
- “Sovereignty and the Role of Government in Cyberspace”, Brown Journal of World Affairs, 16(2): 55-65. Liaropoulos, Andrew. 2017.
- “Cyberspace Governance and State Sovereignty”, in Democracy and an OpenEconomy World Order, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are major challenges on formulating international law on cyberspace?**

There are three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

1.10 ACTIVITY

Explain the legal framework of cyberspace under international law along with its jurisprudential perspective. (Word count 2000 to 2500)

Unit 2: THE CUSTOMARY INTERNATIONAL LAW OF CYBERSPACE

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Development of law through Custom of Cyber

2.4 Let's sum up

2.5 Further reading

2.6 Check your progress: Possible Answers

2.7 Activity

2.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Historical background of customary practice and how it has affected the cyberspace regulation.
- The international norms which governs cyber laws in various jurisdictions.

2.2 INTRODUCTION

International law's applicability to cyberspace and cyber activities has been a source of debate. The highly contested topic was whether cyberspace provides a new "Wild West" in which current international law standards, if not international law itself, would be inapplicable and therefore would not govern actions taking place in this "space." Both scholarly research and state practice have agreed that international law extends to cyberspace and cyber operations. This was acknowledged in the UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) reports in 2013 and 2015, and several States confirmed this position in their comments to the UN Secretary-General and in their national cyber defense and cybe security plans. As a result, the focus shifted to deciding how international law principles could be interpreted and applied to cyberspace and cyber operations. This does not, however, imply that applying international law norms is straightforward. On the opposite, there are significant concerns over how to perceive and enforce a number of standards. In this regard, there are two key challenges: on the one hand, due to the special characteristics of cyberspace, interpreting the application of international law to cyber operations may necessitate any adaptation. In the other hand, international law topics, especially States, may have differing, if not divergent, views of basic international law norms.

The first thing to understand about international law is that it bears just a passing similarity to the law that most people are familiar with. In most nations, domestic laws are enacted by a sovereign body (such as Congress) after careful thought. Statutes are meticulously designed to ensure that the legislation has a specific

effect. This is not the case for international law. Treaties are not the principal means of defining international law, contrary to common opinion. International law is a jumble of historical experience and history, as well as negotiated treaties between countries. Under this patchwork of rules, customary international law—rather than laws or conventions—takes precedence in emerging areas of the law.

When states adopt their general and compatible practices out of a sense of moral responsibility, customary international law evolves. When this happens, nation-states deem customary law to be legally binding. Nations can take measures they consider necessary in situations where there is no existing consensus on what constitutes lawful conduct. The Lotus philosophy, so named after the International Court of Justice decision in which it was created, is based on this. Just a few acts are called peremptory conventions of international law, meaning they are generally considered to be wrong and illegal. Piracy, child trafficking, and hijacking are examples of exemplary regions. The international legal system's very existence is one of the reasons there are so few widely recognized standards.

It is determined by what nations do and feel they are obligated to do, which makes reaching a consensus impossible. Except in seemingly simple situations like torture, there is no rule without agreement. Many states regard “torture or unfair, inhuman, or degrading treatment or punishment” as a violation of human rights norms that have become customary international law. Nonetheless, acts resembling torture occur, and states that support them are rarely condemned, so it is impossible to claim that there is full international consensus on the subject.Although the few prohibitions accepted as peremptory norms do not apply to war, this does not mean that armed conflict is unregulated.

There is a body of customary law reflecting the extensive and virtually uniform conduct of nation-states during traditional warfare that is widely accepted and well understood—the law of war. Unfortunately, the application of the law of war to cyberspace is problematic because the actions and effects available to nations and non-state actors in cyberspace do not necessarily match up neatly with the principles governing armed conflict. Cyberspace gives nation-states new options, enabling them to take non-kinetic actions that may not have been available previously. Actions that may have required the use of military force in previous

conflicts now can be done with cyber techniques without the use of force. States can also take actions in cyberspace that would be consistent with the use of armed force but more easily avoid taking responsibility for the actions—they can take cyber action “without attribution.” In the absence of a specific legal regime for cyberspace, the logical approach is to take what guidance exists to govern more conventional warfare and determine whether it can be applied to cyberspace activities. The subsequent brief discussion is a general examination of how national practices become customs binding on the body of nations as customary international law. Following the general discussion is a more detailed discussion of how customary international law might apply to nation-state cyber actions.

Countries' diplomatic affairs are gradually taking place in cyberspace. State and non-state players established policies and moral conceptions that may be considered international customary law in statu nascendi, ranging from questions regarding data protection and Internet monitoring to privacy and malicious expression. The aim of this contribution is to raise evidence in favour of the idea that international law analysis should be expanded to cover cyberspace. Due to the absence of treaty law in this field, one must turn to a secondary source of international law, namely tradition, as noted by one eminent researcher: 'customary law still regulates various branches of international law, and, more importantly, new rules of that law are emerging.'

2.3 DEVELOPMENT OF LAW THROUGH CUSTOM OF CYBER

The increasing use of computers and computer networks through the 1970s and 1980s was followed swiftly by the rise of the "network of networks" known as the Internet in the mid-1990s. Ultimately, the Internet spawned an entirely new domain of operations referred to as cyberspace. It is in and through this virtual space that cyber activities occur. So, not only are the activities in cyber new, where cyber actions take place is a unique location. Because it has existed for such a short time, there is not a robust body of law governing state conduct in cyberspace. There are documented instances of state cyber practice, however, and these have begun to

lay a pattern for establishing customary cyber law.

As noted above, customary law does not instantly appear but is developed through state practice and rationale. The cyber practices of states and the thought behind those actions over the past 30 years must be examined to determine if there is customary law in cyberspace. If no principles have developed, as earlier discussed, cyberspace remains unconstrained under the default customary international regime. Although opinio juris is a critical element, it is easiest to analyze the development of custom beginning with an examination of state action, which is more visible and easily documented than motivation. Complicating the analysis is the secrecy surrounding most cyber operations. The US Department of Defense (DoD), for example, claims it suffers millions of scans and thousands of probes into its networks each day. With rare exceptions, no states or individuals come forward to take credit for these actions, so assessing the motivation of these unknown cyber actors is difficult. Albeit complicated and difficult, a few examples of state practice in cyber are available for examination.

Arguably, the first cyber attack occurred in the Soviet Union. In 1982, a trans-Siberian pipeline exploded. The explosion was recorded by US satellites, and it was referred to by one US official as “the most monumental nonnuclear explosion and fire ever seen from space.”It has been reported the explosion was caused by computer malware the Central Intelligence Agency implanted in Canadian software, apparently knowing the software would be illegally acquired by Soviet agents. Because the explosion happened in remote Siberia, it resulted in no casualties. It also embarrassed the Russian Committee for State Security (the KGB), who thought they had stolen the most recent software technology from the United States. As a result, the facts behind the explosion were concealed, and the USSR never publicly accused the United States of causing the incident.

Multiple “soft” computer attacks occurred against US systems as the Internet grew exponentially over the next 25 years. Many of these involved attempts to copy sensitive information or relatively simple but potentially devastating denial of service attacks.22 Some of the more infamous include Moonlight Maze (1998–2001), which probed government and academic computer systems in the United States; Code Red (2001), which launched a worm intended to conduct a denial of service attack

against White House computers; and Mountain View (2001), a number of intrusions into US municipal computer systems to collect information on utilities, government offices, and emergency systems.

Although there was speculation about the origins, none of these incidents could be definitively attributed to a state actor. In contrast to the, until recently, little-known Siberian incident, it was a very public series of cyber events considered by many to have heralded the advent of cyber warfare. In April 2007, following the removal of a Russian statue in Estonia's capital of Tallinn, a widespread denial of service attack affected its websites. As a result Estonia, one of the world's most wired countries, was forced to cut off international Internet access. Russia denied involvement in the incident, but experts speculate the Russian Federal Security Service (FSB) was behind the distributed denial of service event.

The following year, Russian troops invaded the Republic of Georgia during a dispute over territory in South Ossetia. In August 2008, prior to Russian forces crossing the border, Georgian government websites were subjected to denial of service attacks and defacement. While there is widespread belief the incident was "coordinated and instructed" by elements of the Russian government, no one has been able to attribute these actions definitively to Russia.

The wakeup call for the US military occurred in 2008, although the details did not become public until two years later. Operation Buckshot Yankee was the DoD's response to a computer worm known as "agent.btz" infiltrating the US military's classified computer networks. The worm was placed on a flash drive by a foreign intelligence agency, from where it ultimately made its way to a classified network. The purpose of the malware was to transfer sensitive US defense information to foreign computer servers. In what qualifies as bureaucratic lightning speed, US Cyber Command was established less than two years later, with a mission to, among other things, direct the operations and defense of DoD computer networks.

In addition to unmasking the extent of network vulnerabilities, the event highlighted the lack of clarity in international law as it relates to cyber events. Two recent incidents merit attention before discussing the law in depth. In 2010, Google reported Chinese hackers had infiltrated its systems and stolen intellectual property. Through its investigation, Google learned the exfiltration of its information

was not the only nefarious activity; at least 20 other companies had been targeted by Chinese hackers as well. These companies covered a wide range of Google users, including the computer, finance, media, and chemical sectors. The Chinese had also attempted to hack into G-mail accounts of human rights activists and were successful in accessing some accounts through malware and phishing scams. Google released a statement explaining what it discovered through its investigation and what steps it was taking in response to China's action, including limiting its business in and with China.

Also in 2010, a computer worm named Stuxnet was detected on computer systems worldwide. Stuxnet resided on and replicated from computers using Microsoft's Windows operating system but targeted a supervisory control and data acquisition (SCADA) system manufactured by Siemens. Cyber experts determined the worm was designed to affect the automated processes of industrial control systems and speculated that either Iran's Bushehr nuclear power plant or its uranium enrichment facility at Natanz was the intended target. After Stuxnet became public, Iran issued a statement that the delay in the Bushehr plant becoming operational was based on "technical reasons" but did not indicate it was because of Stuxnet. The deputy director of the Atomic Energy Organization of Iran stated, "Most of the claims made by [foreign] media outlets about Stuxnet are efforts meant to cause concern among Iranians and people of the region and delay the launch of the Bushehr nuclear power plant."32 Iranian president Ahmadinejad stated at a news conference that malicious software code damaged the centrifuge facilities, although he did not specifically state it was Stuxnet or the Natanz facility.

2.4 LET'S SUM UP

In this chapter, we have learned the formal international agreements, cyber custom which is beginning to develop through the practice of states. Besides, we have also learned the serious actions against major financial institutions.

2.5 FURTHER READING

- "The analysis of the practice of states before the conclusion of the 1967 Outer Space Treaty shows that historically, custom was the first source of the international law of outer space." Vladelen S. Vereshchetin and Gennady M.

Danilenko, “Custom as a Source of International Law of Outer Space,” Journal of Space Law 13, no. 1 (1985): 22, 25.

- Malanczuk, Akehurst’s Modern Introduction to International Law, 43, n. 10. See I. C. MacGibbon, “The Scope of Acquiescence in International Law,” 1954 British Yearbook of International Law, 143, 145–46; and MacGibbon, “Customary International Law and Acquiescence,” 1957 British Yearbook of International Law, 115, 138.
- Harry Newton, Newton’s Telecom Dictionary, 23rd ed. (New York: Flatiron Publishing, 2007), 502–3.

2.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the difficulty in application of customary cyber laws?**

There is a body of customary law reflecting the extensive and virtually uniform conduct of nation-states during traditional warfare that is widely accepted and well understood—the law of war. Unfortunately, the application of the law of war to cyberspace is problematic because the actions and effects available to nations and non-state actors in cyberspace do not necessarily match up neatly with the principles governing armed conflict.

2.7 ACTIVITY

Explain the detailed account of rise of customary practice in the sphere of cyberspace. (Word count 2000 to 2500)

3

Unit 3:CYBERWARFARE AND INTERNATIONAL LAW

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 How is cyber warfare is unique

3.4 Cyber Warfare and International Humanitarian Law

3.5 Cyber operations, attacks, exploitation and defence

3.6 Cyber operations and Jus ad Bellum

3.7 Cyber operations and the prohibition of interstate force

3.8 Let's sum up

3.9 Further reading

3.10 Check your progress: Possible Answers

3.11 Activity

3.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Historical background of cyberwarfareand its treatment in international law.
- The international norms and United Nations strategy on cyberspace.
- Various governing treaties on cyber-attack across the globe.

3.2INTRODUCTION

Cyber warfare is a hot topic for politicians and military officials all over the world. At all levels of government, including the armed forces, new divisions to ensure cyber security are being established. However, in armed conflict environments, cyber operations may have very significant implications, particularly if their impact is not limited to the data of the targeted information system or computer. Indeed, cyber operations are often meant to have a real-world effect. Manipulation of an enemy's air traffic control controls, oil pipeline flow systems, or nuclear reactors, for example, can be accomplished by tampering with supporting computer systems.Any cyber operations have the potential to have a huge humanitarian effect on civilians. Since one of the key purposes of this body of law is to shield civilians from the consequences of conflict, it is critical to address the principles of international humanitarian law (IHL) that regulate those operations. This essay aims to answer some of the issues that emerge when applying IHL to cyber security. IHL is a body of legislation that was drafted with conventional kinetic warfare in mind. Policymakers and military officials all over the world are concerned about cyber security.The United Nations Institute for Disarmament Research (UNIDIR) recently released a report that explains the actions taken by thirty-three states that have directly used electronic warfare in their military strategy and organization, as well as an analysis of thirty-six other states' cyber defense approaches.

For the purposes of this discussion, “cyberwarfare” refers to warfare carried out in cyberspace using cyber means and methods. Where “warfare” is widely interpreted to refer to the use of military force in times of armed conflict, “cyberspace” can be described as a globally integrated network of digital information and communications infrastructures, which includes the Internet, telephone networks,

computer systems, and the data they contain. Infecting a belligerent adversary's data network with a malicious virus, for example, would be called cyberwarfare, but aerial bombing of a strategic cyber command would not.The fact that cyberwarfare is performed in cyberspace does not rule out the likelihood of physical or other non-electronic consequences happening outside the cyber realm, and the perpetrator may also wish for this to happen. Persons whose lives, or artifacts whose operation is dependent on computer networks, such as certain power stations, modes of transportation, or people attached to different types of medical, military, or technical life-support systems, are examples of cyberwarfare goals.

3.3 HOW IS CYBERWARFARE UNIQUE?

When defining and adapting current international law to cyberwarfare, the unique features of cyberspace must be taken into account. Most importantly, cyberspace is the only fully man-made domain. It is jointly developed, maintained, managed, and run by public and private partners all over the world, and it is continuously changing in response to technical advancement. Since cyberspace has no geopolitical or natural borders, information and electronic payloads can be transmitted from any point of origin to any point of destination through the electromagnetic spectrum.These are transported in the form of numerous digitalized fragments through volatile routes before being reassembled at their destination. Although states, non-state organisations, private businesses, and individuals all have access to cyberspace, IP spoofing and botnets, for example, make it possible to hide the root of an activity, making accurate detection and attribution of cyber attacks especially difficult.

3.4 CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW

There is no unanimously agreed definition of cyber warfare, however there are a few authoritative drafts. The Tallinn Manual 2.0 distinguishes between (a) the means, and (b) the methods of cyber warfare as being: a) cyber weapons and their associated cyber systems; b) cyber tactics, techniques, and procedures by which hostilities are conducted (Tallinn Manual, p. 452). This definition notes that the ‘means of cyber warfare’ include cyber weapons and cyber weapon systems. In this context, a

weapon is the part of the system which causes damage or injury. This broad definition allows for cyber warfare to encompass cyber devices, equipment, or software used, designed, or intended to be used to conduct a cyber attack. Subsequently, it defines cyber weapons as “cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack” (ibid). It states that this definition is applicable to International Armed Conflicts and Non-International Armed Conflicts.

Academics such as Rid and McBurney define cyber weapons as a “computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things” (Ridd, Cyber Weapons p. 7). A third definition is provided by the US Air Force which interprets weapons as “devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or material” (US Air Force Instructions, Legal Review of Weapons and Cyber Capabilities, p. 6). All three definitions have one primary aspect in common: they all agree that cyber weapons are the tools of harm. Consequently, there are a few things which can be deduced about cyber warfare from the above definitions. Firstly, a vast multitude of cyber weapons exists ranging from highly advanced to much more basic. Gone are the days when the worst thing on the Internet to be afraid of was a pesky virus. The current highly sophisticated malware looks for software vulnerabilities which can result in fatal damage to the opponent’s entire computer network. The most advanced cyber weapons are capable of entering networks which are off the grid, causing total damage. Such stateof- the-art weapons are expensive to make as there are not many individuals capable of writing them to such a high standard. On the other hand, a basic cyber weapon is easier to detect as it focuses on denying service to an opponent’s computer rather than targeting the computer directly. Such an attack was conducted by a pro-Kremlin youth group against Estonia in 2007. Secondly, cyber weapons result in different effects. The initial stage affects the targeted computer networks. This results in destruction of the system and impacts persons by for example cutting power to a power plant or locking exit doors. The main difference between cyber weapons and traditional weapons is the sequence of events:

traditional weapons usually cause immediate damage to people, whereas cyber warfare affects people at a later stage.

Indiscriminate cyber weapons

Having provided an explanation of cyber weapons above, it is important to determine whether a weapon is inherently indiscriminate as per the review of a weapon under international humanitarian law (IHL). Indiscriminate cyber weapons are defined as being: a) directed at a specific military objective, or b) limited in the effects as required by law of armed conflict. Consequently, they strike military objectives and civilians or civilian objectives without distinction (Tallinn Manual, p. 455). Criterion (a) highlights the primary principle of IHL to respect the delicate balance between humanitarian considerations and military necessity. IHL focuses on protecting civilians from attacks. Therefore, the weapons need to be as accurate as possible to limit the risk of harm. From what can be gathered, powerful States are meeting or have met the requirement in (a) in terms of their cyber warfare. As technology advances, an increasing number of States will be able to fully fulfil this requirement. On the contrary, criterion (b) involves effects that are not limited. As per the Manual, here is a sequence of events which breach (b) as the effects cannot be limited: 1. A State uses malware against another State in an armed conflict; 2. The malware is targeting military computer networks; 3. Even though the intended target is military, the malware will unavoidably spread into the civilian networks (Cyber Weapons Reviews under International Humanitarian Law 'Tallinn Paper no 11', p. 19). The above scenario demonstrates the unintentional simplicity in breaching (b). Therefore, there are two subparts to (b) to make it fit in the IHL framework. Firstly, the effects need to be harmful and cause injury to persons or damage to property. Secondly, the indiscriminate effects must be foreseeable.

IHL will only be applicable to a cyber warfare occurrence if the attack occurs during or triggers an armed conflict. It is questionable whether a cyber attack can constitute the 'use of force' or an 'armed attack' in order for IHL to apply. Furthermore, attributing the attack to a State or an armed group poses questions which take time to be answered, whilst on the other hand IHL cannot wait until it is determined whether the cyber attack qualifies as such or not. There is a need for more adherent rules which encompass non-physical armed attacks to reflect the changing

weaponry of the 21st century. The Tallinn Manual makes useful suggestions, but still has a long way to go to place cyber warfare in the IHL framework.[76]

3.5 CYBER OPERATIONS, ATTACKS, EXPLOITATION AND DEFENCE

The reduction of information to electronic format and the subsequent transfer of that information between physical elements of cyber infrastructure is referred to as “cyber activity” or “computer network operation” (CNO). “Computer network attack,” “computer network exploitation,” and “computer network defense” are the three types of cyber operations.Computer network attacks (CNA) refer to any cyber operations aimed at “disrupting, denying, degrading, or destroying information resident in computers and computer networks, or the computers and networks themselves,” while computer network exploitation (CNE) refers to “enabling operations and intelligence gathering to gather data from target or adversary automated information systems or networks.” Computer network defence CND, on the other hand, refers to “measures taken to secure, track, analyze, identify, and respond to unauthorized activity within... information systems and computer networks,” or, in other words, the prevention of CNA and CNE using surveillance, counterintelligence, law enforcement, and military resources. This vocabulary, which is unique to cyberspace activities, must be distinguished from other technical words used in international law, such as “force,” “armed attack,” and “attack.”

3.6 CYBER OPERATIONS AND JUS AD BELLUM

The jus ad bellum is the body of law governing the use of force by states in international relations. The UN Charter is the most important source of jus ad bellum today. Such facets of the rule, such as the particular modalities regulating the use of force in self-defense, are not covered by the UN Charter and must be drawn from customary law as expressed in state procedure and opinio juris, as well as defined in international jurisprudence.In this case, it would be appropriate to determine if cyber operations constitute (1) a globally wrongful threat or usage of “force,” (2) a “armed assault” justifying the use of necessary and proportionate force

[76] https://leidenlawblog.nl/articles/cyber-warfare-the-definition-challenge

in self-defense, or (3) a “threat to the peace,” “breach of the peace,” or “act of aggression” requiring UN Security Council action.

In fact, the first issue is important because state-sponsored cyber operations that count as a use of “force” against another state would not only violate the UN Charter's general prohibition of “force,” but would also likely lead to a foreign military conflict. In the other hand, cyber operations below the threshold of “force,” even if otherwise forbidden under the customary principle of non-intervention, can constitute lawful counter-measures in response to foreign wrongful actions that do not meet the threshold of “armed attack” by another state.The second issue is important because the existence of cyber operations that constitute a “armed assault” allows the targeted state to exercise its inherent right to self-defense by means that are otherwise forbidden by the Charter, such as the use of force.

Finally, assessing that cyber operations are a “danger to the peace,” “breach of the peace,” or “act of aggression” requires the UN Security Council to take punitive action, including military force, to preserve or restore internal peace and security, regardless of whether the cyber operations in question are categorized as “force” or “aggression.”

3.7 CYBER OPERATIONS AND THE PROHIBITION OF INTERSTATE FORCE

Cyber Operations as “Force”

“All Members [of the United Nations] shall refrain in their foreign affairs from the threat or use of force against the territorial integrity or political freedom of any entity, or in any other manner inconsistent with the United Nations Purposes,” according to article 2(4) of the UN Charter. As a result, the issue of whether cyber operations count as “force” under the scope of this prohibition emerges.

In the absence of a treaty formulation, the principle of “power” must be understood in good conscience in terms of the Charter's object and intention and the ordinary interpretation to be assigned to the word in its sense. Despite the fact that the ordinary sense of “force” is obviously broad enough to encompass both armed and unarmed means of coercion,18 the vast majority of observers today regard the

word “force” in UN Charter article 2(4) as literally interchangeable with “armed” or “military” force. This does not imply that the ban against the use of kinetic, toxic, biochemical, or nuclear weapons is exclusive to such weapons.The ban extends “to all use of force, regardless of the weapons used,” according to the International Court of Justice.

Indeed, once the results of cyber operations are equal to those likely to arise from kinetic, toxic, biochemical, or nuclear weaponry, they come under the prohibition of article 2(4) of the UN Charter. This will undoubtedly entail the use of cyber operations as an offensive or defensive weapon to inflict death or injuries to people, as well as the destruction of artifacts and facilities, whether the destruction be caused by physical damage, technical harm, or a combination of the two.

Cyber operations manipulating target computers systems to trigger a meltdown in a nuclear power plant, or opening the floodgates of a dam over a densely populated area, or disabling a busy airport's air traffic control during bad weather conditions, are both obvious examples of a use of “force” within the meaning of article 2(4) of the UN Charter. The main issue is determining whether cyber operations that do not, or do not explicitly, cause death, damage, or destruction qualify as a use of “force.”The UN Charter's preparatory works explicitly demonstrate that the prohibition of “power” did not apply to economic exploitation or political pressures. Furthermore, article 41 of the UN Charter defines “interruption of... communication” as a “measure not requiring military force,” implying that any denial of service attacks (DOS) will be exempt from article 2's prohibition (4). This does not, however, imply that all cyber activities fall short of military force in the absence of violent consequences.

Although one early commentator suggested a complicated set of indicative criteria for distinguishing between military force and economic or political exploitation in the cyber domain, others have recently pointed out qualitative, quantitative, and temporal flaws in these criteria, highlighting rather than removing the ongoing lack of clarification in this region.From a teleological standpoint, it is arguable that the Charter can only achieve its overarching goals of maintaining international peace and security (article 1) and “saving succeeding generations from the scourges of war” (preamble) if it prohibits the use of any forcible measure likely to provoke

military counter-force and, ultimately, the outbreak of international armed conflict.

The Charter cannot, by logic, authorize the ban of interstate force to be circumvented by the use of nonviolent means and approaches that are, for all intents and purposes, equal to a violation of the peace between the parties. Consider the debilitating impact of cyber operations causing the failure of large cities' electrical power supplies, the incapacitation of networks regulating factory activity, or the penetration of malware intended to “blind” a whole air defense infrastructure. In this sense, it's worth noting that UN Charter article 2(4) forbids the use of force between states, regardless of its extent or size.Also small acts of interstate force, as the International Court of Justice (ICJ) explained in the Nicaragua Case, come under the general prohibition of article 2(4) of the UN Charter, regardless of whether they count as acts of “aggression” or “violent assaults,” allowing the threatened state to use force in self-defense. This view is supported by the position taken in International Humanitarian Law, which holds that even small acts of military action between states are necessary to initiate an international armed conflict.Indeed, it would be illogical for article 2(4) of the UN Charter, as the primary standard aimed at ensuring international peace and stability, not to routinely ban all kinds of interstate behavior necessary to trigger an international military conflict within the scope of article 2 of the Geneva Conventions, as the primary norm aimed at ensuring international peace and security. In fact, the UN Charter goes even further, prohibiting not just the direct use of force in interstate affairs, but also the threat of force.

3.8 LET’S SUM UP

In this chapter, we have learned the formal international agreements, cyberwar fare and its essentials. Additionally, we have also learned how UN has tried to formulate the strategies to curb cybercrime.

3.9 FURTHER READING

- For the ICRC’s position on this issue see Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL, ICRC, 2009, § II.

See also Prosecutor v. Martić, judgement of 8 October 2008, ICTY, §§ 300–302.

- Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, vol. I, 2005, p. 19.
- Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL, ICRC, 2009, p. 22.
- Marco Roscini, "World Wide Warfare—Jus ad bellum and the Use of Cyber Force", in Armin Bogdany and Rüdiger Wolfrum (eds.), Max Planck Yearbook of United Nations Law, vol. 14, 2010, p. 96.
- Michael Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", Naval War College International Law Studies, 2011, p. 8; Michael Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", International Review of the Red Cross, vol. 84, no. 846, 2002, p. 381.

3.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber operation?**

The reduction of information to electronic format and the subsequent transfer of that information between physical elements of cyber infrastructure is referred to as "cyber activity" or "computer network operation" (CNO). "Computer network attack," "computer network exploitation," and "computer network defense" are the three types of cyber operations.

3.11 ACTIVITY

Explain the detailed account on UN strategies and related provisions on cyber-attack and security. (Word count 2000 to 2500)

4

Unit 4: INTERNATIONAL COURTS FOR CYBERSPACE

4.1 Learning Objectives

4.2 Existing International Courts

- 4.2.1 International Court of Justice
- 4.2.2 Internal Criminal Court
- 4.2.3 The International Criminal Tribunal for the former Yugoslavia

4.3 Role of the judges in International courts

4.4 Let's sum up

4.5 Further reading

4.6 Check your progress: Possible Answers

4.7 Activity

4.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- Various international courts handling the matters related to cybercrime and related matters.
- Provisions governing the jurisdictions of these courts.
- Role of judges in these courts.

4.2 EXISTING INTERNATIONAL COURTS

4.2.1 The International Court of Justice

The Court was established in the early 1900s, based on the 1899 and 1907 Hague Peace Conventions. In 1913, it was renamed the Permanent Court of Arbitration and relocated to The Hague's Peace Palace, which was funded by Andrew Carnegie's contributions. The Permanent Court of International Justice was created by the League of Nations after World War I, but it was never a member of the League. The Court ceased to exist after World War II broke out, but convened for the last time in October 1945. The International Court of Justice was created by the United Nations Charter, which stipulates that all UN members be parties to the Courts Statute.The Court, which began operations in 1946, is the United Nations' primary judiciary body. The International Court of Justice serves as a global tribunal. The Court is made up of 15 judges who are chosen for a nine-year term by the United Nations General Assembly and the Security Council, who sit separately. No country may have more than one judge, and one-third of the judges are elected every three years. A State party to the case can select an ad hoc judge for the case's purposes.The Court's authority is as follows: The Court resolves legal cases that are referred to it by consensus with the parties to the lawsuit, in compliance with international law. Only the United Nations' organs and 16 specialist organizations with the authority to make such a request will request advisory opinions on legal issues from the Court. If there are any questions regarding the authority, the Court will rule. The decisions are final and irreversible.

4.2.2 The International Criminal Court

The promise of universal justice lies in the prospect of an international criminal court. 1 Many serious cyberattacks will go unpunished without an international court or tribunal to deal with the most serious cybercrimes of global concern. The most extreme global cyberattacks of the last year have shown that virtually no one has been investigated, convicted, or punished for their actions. Such crimes must be covered by a worldwide convention or series of treaties, and they must be investigated and tried by an international criminal court or tribunal.After ground, sea, air, and outer space, cyberspace is the fifth shared space in need of international collaboration, cooperation, and legal steps. The international community must be made aware of the need for a global solution to the immediate and growing cyberthreats. International law shall protect peace, justice, and stability in cyberspace by a treaty or series of treaties under the United Nations. The rapid evolution of global cyberattacks, such as large and orchestrated attacks against sovereign states' sensitive intelligence infrastructures, necessitates an immediate response in the form of a global treaty.

The United Nations has launched a thorough investigation into the issue of cybercrime. The 12th United Nations Congress on Criminal Prevention and Criminal Justice, held in Salvador, Brazil in April 2010, requested that the UN Commission on Crime Prevention and Criminal Justice convene an open-ended intergovernmental advisory committee to conduct a thorough report on the issue of cybercrime and its solution in Article 42 of the Salvador Declaration. The Commission and the United Nations General Assembly both approved the recommendation in resolution 65/230.The aim of this systematic report is to look at the issues “in order to explore options for strengthening existing and proposing new national and international legal or other solutions to cybercrime.”

The Court was founded in 1998 at a conference in Rome by 120 countries. The International Criminal Court's Rome Statute was introduced and went into effect on July 1, 2002. 111 countries have ratified or acceded to the Rome Statute. While the Court is not affiliated with the United Nations, it has historical, legal, and organizational links to the organization. The Rome Statute and other contract arrangements control the relationship. The International Criminal Court (ICC) is the

world's first permanent, treaty-based, entirely autonomous international criminal court, established to promote the rule of law and ensuring that the world's worst criminals are not forgotten.The Court's authority is just a supplement to national criminal authorities, not a replacement for them. If a State party to the Rome Statute refuses or is reluctant to sue, it may investigate and prosecute. Anyone who violates any of the Statute's provisions will face legal action by the Court. The International Criminal Court's authority is limited to States that become Parties to the Rome Statute, but certain States are expected to completely participate in the investigation and trial. Article 5 restricts the scope of the court's jurisdiction to the most serious offences that affect the international community as a whole. The article explains the jurisdiction, which includes genocide, crimes against humanity, war crimes, and violence. Individual states may refuse to are unable to exercise authority in a particular case.

According to article 17, a State is unable to report or prosecute a crime if there seems to be a real lack of will to do so. When a state's justice system tends to be in complete or significant failure, or when it is unable to procure the accused or the requisite proof and witnesses for any reason, or when it is otherwise unable to carry out its prosecutions due to its unavailability, the state is unable. Other extreme crimes, such as terrorist attacks, were debated at the final diplomatic conference in Rome, but the conference regretted that no universally accepted concept could be reached.Terrorism attacks are serious offences that concern the international community, and the conference agreed that a study conference convened under Article 123 of the Statute of the International Criminal Court deem them for inclusion in the list of offenses subject to the Court's jurisdiction. In 2010, the Court was summoned in five instances. Uganda, the Democratic Republic of Congo, the Central African Republic, Sudan's Darfur, and Kenya are all affected. Furthermore, the lawyer is pursuing preliminary inquiries in a variety of other countries around the world.

Also in the new authority, the International Criminal Court may have a part to play in the war against terrorism. The Court can, upon request, “cooperate with and provide assistance to, a State Party undertaking an investigation into or prosecution in respect of conduct that constitutes a crime under the jurisdiction of the Court, or that constitutes a serious crime under the national law of the requesting State.”

Terrorism is unquestionably a “violent crime.” Massive and organized cyber attacks on information infrastructures can still be deemed a “violent crime,” even though they aren't considered terrorism.The Kampala Review Conference took place from May 31 to June 11, 2010. The Conference drew about 4600 delegates from states, intergovernmental bodies, and non-governmental organizations. The International Criminal Court was now fully functioning as a legal organ, and the Meeting was formally opened by the Secretary-General of the United Nations. The Rome Statute was amended, with the addition of a description of the crime of violence. The Kampala Declaration was also adopted, with section 12 reading, “Decide to observe 17 July, the day of the adoption of the Rome Statute in 1998, as the Day of International Criminal Justice from now on.”

- ***The rule of law on the most serious crimes in cyberspace***

The institutional convergence of procedural and court cases on terrorism and other serious offences in cyberspace may be strengthened by a binding global legislative instrument like the International Criminal Court's Rome Statute. The Rome Statute may provide a global judicial system to ensure that certain actions are not excluded from effective sanctions. If criminal actions or terrorist use of the Internet, as well as huge and coordinated multinational activities in cyberspace, the Rome Statute has Articles on investigation, indictment, and three branches of Courts for regular and structured prosecutions.However, the Prosecutor, as an impartial arm of the Court, can, after evaluating the evidence provided, launch an investigation on a case-by-case basis. (Articles 18 and 53) Under Article 18 on provisional decisions on admissibility, the Prosecutor can “seek permission from the Pre-Trial Chamber to take appropriate investigative action for the purpose of maintaining evidence where there is a one-of-a-kind opportunity to acquire critical evidence or where there is a serious risk that such evidence will not be available later.”Such a unique procedure could be used in the investigation of terrorist threats and large-scale, coordinated cyberattacks. That is also the Pre-Trial Chamber that issues an arrest warrant later on. The Court can exercise its duties and powers on the territories of all States Parties to the Rome Statute, with a maximum penalty of 30 years in prison and the possibility of a life sentence.

4.2.3 The International Criminal Tribunal for the former Yugoslavia (ICTY)

The Tribunal is a United Nations court of law, established under the United Nations Charter's Chapter VII. On May 25, 1993, the Security Council passed Resolution 827, which created the Tribunal.The Tribunal's mandate is to try crimes committed in the former Yugoslavia since 1991, and it has jurisdiction over the following issues:

- Grave violations of the 1949 Geneva Conventions
- War crimes
- Genocide
- Crimes against humanity

In contrast to national courts, the Tribunal has concurrent power, but it has the authority to assume primacy and take over inquiries and prosecutions at any time. The Chambers are made up of 16 permanent judges and up to nine ad hoc judges, all of whom are appointed by the UN General Assembly. Three Trial Chambers and one Appeals Chamber include the judges. The judges are chosen for a four-year term.

The courts have guaranteed a fair and open hearing by weighing the facts in order to assess the accused's guilt or innocence. The Tribunal has demonstrated that effective and transparent international justice is possible, as well as setting significant international criminal and humanitarian law precedents. The Appeal Chamber is made up of seven permanent judges, five from the International Criminal Tribunal for the Former Yugoslavia and two from the International Criminal Tribunal for Rwanda (ICTR).The ICTR's Appael Chamber is made up of the same seven judges, but each appeal is heard and determined by five judges. Since the Nuremberg and Tokyo tribunals, the Tribunal becomes the first major war crimes tribunal.

In the disputes, the Tribunal has prosecuted and filed complaints against people of all ethnic backgrounds. The Prosecutor's Office is independent of the Security Council, every State or foreign body, and the ICTY's other organs. On the basis of evidence obtained, the Prosecutor initiates investigations at his or her discretion. Before an indictment may take effect, it must be approved by a magistrate. The

convicted are being detained in The Hague's ICTY Detention Unit.The maximum sentence that may be imposed is life imprisonment. Sentences are carried out in one of the countries that has concluded a deal with the UN. The judges also have regulatory responsibilities, such as drafting and adopting legislative documents that govern the Tribunal's operations.

4.3 THE ROLE OF JUDGES IN INTERNATIONAL COURTS

The role of judges in upholding the rule of law and human rights in cyberspace must be driven by the fundamental principles for judges outlined in the Consultative Council of European Judges' (CCJE) Magna Carta of Judges, which was adopted on November 17, 2010. The basic principles relating to judges and the legal system are contained in this Magna Carta of Judges, which is strongly recommended as global principles incorporated in a global Treaty.In a national and international context, these fundamental principles include criteria for the rule of law, judicial independence, access to justice, and ethical and responsibility principles. According to section 23 of the Magna Carta, these rules extend mutatis mutandis to judges of both European and foreign courts.The following is the description of the rule of law and justice in section 1:

Any democratic state's judiciary is one of the three branches of government. Its mission is to guarantee the Rule of Law's very survival and, as a result, the law's correct enforcement in an objective, just, equitable, and effective manner. Section 2 explains the main precept of judicial independence: “Judicial independence and impartiality are basic prerequisites for the administration of justice.”

4.4 LET’S SUM UP

In this chapter, we have learned the jurisdiction and limitations of international courts in matters related to cyber security and related aspects.

4.5 FURTHER READING

- Wilson, Clay: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for US Congress (November 2007).
- Sofaer and Goodman: Cyber Crime and Security - The Transnational Dimension of Cyber Crime and Security (2008).

- Sieber and Brunst: Cyber terrorism and Other Use of the Internet for Terrorism Purposes – Threat Analysis and Evaluation of International Conventions (2007).

4.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Explain Article 5 of ICJ.

Article 5 restricts the scope of the court's jurisdiction to the most serious offences that affect the international community as a whole. The essay explains the jurisdiction, which includes genocide, crimes against humanity, war crimes, and violence. Individual states may refuse to are unable to exercise authority in a particular case.

4.7 ACTIVITY

Provide a detailed account on role of International court of justice on cyber crimes.(Word count 2000 to 2500)

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

BAOU
Education for All

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-202
Intellectual Property Rights in Cyber Space

Post Graduate Diploma in

Cyber Law

(PGDCL)

2021

Intellectual Property Rights in Cyber Space

Dr. Babasaheb Ambedkar Open University

Intellectual Property Rights in Cyber Space

Course Writer

Ms. Shivani Jadhav	Research Associate, Gujarat National Law University
Ms. Ambika Batas	Research Associate, Gujarat National Law University
Ms. Dhanya	Assistant Professor (Research), Gujarat National Law University

Content Reviewer

Mr. Kumar Gaurav	Chanakya National Law University, Patna, Bihar

Content Editor

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. 2021

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr.Babasaheb Ambedkar Open University

PGDCL-202

Intellectual Property Rights in Cyber Space

Block-1: Interface of Intellectual Property Rights And Cyber Space

UNIT-1
Intellectual Property Rights Vis-À-Vis Cyber Space 02

UNIT-2
Usage of Internet and The Evolving Challenges of IPR Issues in India 13

UNIT-3
Cyberspace−Conflicting Jurisdictional Spheres of IPR 21

UNIT-4
Cyber security and The Theft of Intellectual Property Online 30

Block-2: Copyright and Cyber Law

UNIT-1
Copyright in Cyberspace 41

UNIT-2
Copyright and Infringement in Cyberspace 50

UNIT-3
E-Commerce & Its Copyright Issues 58

UNIT-4
Copyright Protection in Cyberspace - A Comparative Study Of USA and India 70

Block-3: Trademark and Cyber Law

UNIT-1
Trademark Trafficking in Cyberspace 80

UNIT-2
Infringement of Trademark in Cyber Space 90

UNIT-3
Trademark Law in Cyberspace: Protection to Internet Address 99

UNIT-4
Domain Names, The Internet, and Trademarks 109

Block-4: Emerging Issues in Relation to IPR and Cyberspace

UNIT-1
IPR Management: Emerging Cyberspace Issues in Knowledge Society: A Critical Analysis 119

UNIT-2
Challenges to Copyrightable Work in Cyberspace 130

UNIT-3
Private International Law and Intellectual Property Rights on The Internet 147

UNIT-4
Intellectual Property, Cyberspace and International Law 160

Block-1

INTERFACE OF INTELLECTUAL PROPERTY RIGHTS AND CYBER SPACE

Unit 1: INTELLECTUAL PROPERTY RIGHTS VIS-À-VIS CYBER SPACE

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Interface of Cyber Law with Copyright Law

1.4 Interface of Cyber Law with Trademarks and Domain Names

1.5 Cyber squatting

1.6 Dispute Resolution in Cyber Law

1.7 Conclusion

1.8 Let’s sum up

1.9 Further reading

1.10 Check your progress: Possible answers

1.11 Activity

1.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand

- Interrelationship between intellectual property rights and cyber law
- The concept of Cybersquatting and its impacts
- Dispute resolution in cyberspace

1.2INTRODUCTION

The rapid evolution of cyberspace over the last decade owing to the extensive growth of e-commerce and e-governance on digital platforms has resulted in establishing its unforeseen inter-relationship with a varied range of disciplines, the most significant of them being law. Content which is in the electronic form and can be represented as electronic record are at the epicenter of this Information Technology Ecosystem. With the mass increase in the use of cyber space, availability of content (electronicform) across digital platforms increased by many folds; innovation gave rise to the creation of original and novel content, and intellectual property was disseminated overcoming all geographical boundaries. Cyberspace being a tool of access to data and resources, it expanded human reaches towards global information. As a result, there developed an undeniable relationship between cyberspace and the intellectual property in the content available on the cyberspace.

However, while on one hand, content of various kind including elements of copyright, trademark and patent became easily available to one and all across digital platforms, on the other, there arose instances of violation of intellectual property owing to theft of such content which in turn resulted in complications of piracy and infringement of the rights accruing from such intellectual properties.[1] Consequently, the necessity of protecting digital content was acknowledged, and accordingly, the legal framework of Cyber Law was established to address all concerns of misuse and misappropriation of intellectual property on cyberspace. Apart from the changes in Cyber Law, amendment has been brought in the existing Intellectual Property Laws to make it

[1]Somu, C.S.. (2006). Intellectual Property Rights In Cyberspace. Paradigm. 10. 62-68. 10.1177/0971890720060110.

compatible to digital platforms as well as digital contents. Nevertheless, the necessity of constantly adopting technological measures towards the protection of content available on digital platforms became all the more significant with the strengthening impact of cyberspace on the society and its growth.

Intellectual property is fundamentally associated with territoriality, while cyberspace cannot be restricted within territorial boundaries. As a result of intellectual property being available on cyberspace, the inherent nature of intellectual property underwent an evolution, thereby giving rise to newer interpretations of both cyberspace and intellectual properties. As it is evident from existing statute on cyberspace considerably lacks due attention A major portion of the concept of cyber law hence needs to be studied in context of its association with intellectual property rights.

1.3INTERFACE OF CYBER LAW WITH COPYRIGHT LAW

Cyberspace provides to copyright law a platform to promote and channelize its objectives and purposes, the most significant of which is to provide to the society access to knowledge for establishing overall societal advancement. The intrinsic philosophy of copyright law is aimed at fostering creativity and innovation which the copyright owner and/or holder may subject to commercial exploitation; and cyberspace served as the perfect medium for fulfilling such purposes.[2]

Notwithstanding the positive impact of the internet on copyright law, there is no denying that owing to the inherent nature of copyright law, it has suffered extensively as a result of exposure to emerging technologies, especially the growth of cyberspace. The very structure of cyberspace and its inherent characteristics has a dual impact on the copyright regime. Both positive impact and negative impact can be easily found the in distribution, reproduction and its exploitation/accessibility of copyright material. While distribution, reproduction and exploitation of copyrighted material have found new direction through cyberspace and content has become easily accessible, it has also adversely affected the copyright holders. Not only does the internet eliminate all distinction between private and public use, but it also creates complications towards the interpretation of use of copyrighted materials

[2]A. Rahmatian, (2015) 'Cyberspace and intellectual property rights', in: Tsagourias, N. T. and Buchan, R. (eds.) Research Handbook on International Law and Cyberspace (Cheltenham: Edward Elgar), 2015, pp. 72-93 (chapter 4)

thereby diluting the grounds of copyright infringement. The fundamentals of the copyright law state that infringement shall be deemed to have occurred if the exclusive rights of the copyright owner are exercised without express authorization of the owner or right-holder. Since the copyright law validates the use and/or reproduction of copyrighted material for personal/private use, it is essential to understand whether copyrighted content has been subjected to private use or not for determining the occurrence of infringement. However, cyberspace has introduced digital technology that has allowed merging of private and public spheres into one; as a result of which, copyright owners have failed to effectively exercise control over the use of their content and have often failed to prevent unauthorized exploitation of the same. Digital technologies introduced by cyberspace include all forms of copyrightable content that might inter alia include texts, graphics and images, which may be combined in various forms to generate new content.[3]

The reproduction and display of a copyrighted work of another person, in a non-removable or removable storage medium, without his authorization amounts to an infringement of statutory exclusive rights vested in the said copyright owner.

In *Kelly v Arriba Soft Corp.*[4]*,* the plaintiff, Leslie Kelly, a professional photographer who had copyrighted many of his images of the American West. Some of these images were located on Kelly's website or other websites with which Kelly had license agreement. The defendant, Arriba Soft Corp. operated an Internet search engine that displayed its results in the form of small pictures rather than the more usual form of text. Arriba obtained its database of pictures by copying images from other websites. By clicking on one of these small pictures, called *'thumbnails'*, the user could view a large version of that same picture within the context of the Arriba web page. The circuit court held that *"the creation and the use of the thumbnails in the search engine is a fair use, but the display of the larger image is a violation of Kelly's exclusive right to publicly display his works.*

As opposed to the primitive system of dealing with physical copies of copyrighted content which allowed right-holders to keep track of the use of their copyrighted materials, cyberspace has introduced a system that allows unprecedented replication, spread, reproduction and sale of content within mere seconds without

[3]Bently, Lionel and Sherman, Brad (2009), Intellectual Property Law, 3rd ed., Oxford: Oxford University Press

[4] 280 F. 3d 934 (9th Cir 2002)

adversely affecting the quality of such content. As a result, the market for such copyrighted content gets hampered, as does the copyright owners' right to share the revenues accrued from exploitation.

1.4INTERFACE OF CYBER LAW WITH TRADEMARKS AND DOMAIN NAMES

Trademarks, as commonly understood are marks representing goods and/or services or chains thereof graphically or otherwise, thereby allowing consumers to identify goods and services as well as distinguish between goods and services of similar nature and kind. The Trademarks Act, 1999 aims at acknowledging the rights of registered trademark owners and restricting fraudulent exploitation of the goodwill of one chain of goods/services by another similar chain. One of the basic functions of trademark from the perspective of owner is to protect his goodwill in the market and from the customer's/user's perspective it enables them to distinguish goods and services in the market. However, the evolution of cyberspace has given rise to ample scope of misuse of such trademarks by unauthorized parties which in turn has resulted in misleading consumers and violating the rights of the original trademarks.[5]
In *Uniply Industries Ltd. V Unicorn Plywood Pvt. Ltd.*[6], the Supreme Court has laid down test to determine continuous prior use for grant of temporary injunction in trade mark related cases. It has been observed that, *'some courts indicate that even prior small scale of goods with the mark are sufficient to establish priority, the test being to determine continuous prior user and the volume of sale or the degree of familiarity of the public with the mark. Bona fide test of marketing, promotional gifts and experimental sales in small volume may be sufficient to establish a continuous prior use of the mark.*
Domain names have become a kind of *'e-commerce marks'* in the online medium. These are digital business addresses – a point of business contact or transaction. Domain names provide a system of easy-to-remember Internet addresses, which can be translated by the Domain Name System (DNS) into the numeric addresses (Internet Protocol (IP) numbers) used by the network.

[5]Drahos, Peter (1996), A Philosophy of Intellectual Property, Aldershot: Ashgate
[6] (2001) 5 SCC 95.

The inter-relationship between trademarks and cyberspace was developed in exclusive association with the concept of domain names.[7] In simple words, domain names represent the IP address used in surfing the world wide web. It is owing to use of domain names on cyberspace that the strictly territorial nature of trademarks has now broadened to become global. While on one hand such domain names may refer to internet based digital platforms associated with certain goods and/or services and in turn substantiate the commercial prospects of online businesses, on the other, they would be indicative of the identity, goodwill and quality complimenting such goods and/or services. Evidently, misappropriation of domain names could not only cause immense damage to the business of infringed chain of goods/services, they could completely destroy the goodwill associated with such brands which may have taken ages to build.[8] Additionally, domain name registrations being done on a 'first come first served' basis, there are various instances of fraudulent registration of domain names whereby the party registering, in spite of having no legitimate interest in the brand, deliberately infringed the rights of the original trademark owners to acquire registration in an unauthorized manner. Infringement of trademarks through abuse of domain names on cyberspace is hence a very serious concern for flourishing trades and businesses.

1.5CYBERSQUATTING

Cybersquatting, which literally means 'sitting on another person's property', may be described as instances of fraudulent use and misappropriation of domain names which involve exploitation of online identities of brands that result in violation of rights of the original right-owners. Cybersquatting often give rise to situations wherein parties who have no legitimate rights in certain trademarks get domain names registered in their names and subsequently sell those to the original owner or other parties at exorbitant prices. It may be done inter alia with the intent of preventing the original owner of brands from having access to such domain names, diverting the traffic off the cyberspace associated with the websites of competing brands, and

[7]Drahos, Peter (2002), 'Developing Countries and International Intellectual Property Standard-Setting', 5(5) The Journal of Wold Intellectual Property, 765-789

[8]Easton, Catherine R. (2012), 'ICANN's core principles and the expansion of generic top-level domain names', 20(4) International Journal of Law and Information Technology, 273-290

selling such domain names to earn profits. Evidently, cybersquatting has the potential to cause activities leading to cyber wars.

In India, there is no statutory provision to prevent cybersquatting; however, certain provisions of the Trademarks Act, 1999 are broad enough to address such issues. Cybersquatting can be protected within the legal framework of 'passing off' which emerges from common law principle. Consequently, any person lodging a complaint against cybersquatting necessarily involves the mandate of establishing the following –

a) Dishonest intention of the fraudulent party
b) Absence of legitimate rights being held by the fraudulent party
c) Similarity between the domain name fraudulently registered and the trademark owned by the authentic right-holder

The first Indian case that extensively discussed issues of domain name disputes vis-à-vis cybersquatting was *Yahoo Inc. v Akash Arora (78(1999) DLT 285),*[9] wherein, the defendant contended having used a common dictionary word and having provided a disclaimer in the website with the intention to avoid confusion being created with the plaintiff's website which was registered in more than 69 countries. However, the court held that despite such disclaimers, there would be necessary associations made with the original website of yahoo which was based in a well-known and distinct trademark. Subsequently, in the case of *Tata Sons Ltd. &Anr.v. ArnoPalmen&Anr,*[10] the Delhi High Court dealt with a landmark case on domain name disputes and cybersquatting. The plaintiffs sought permanent injunctions against the defendant's use of the domain name 'www.tatainfotech.in' or such domain names deceptively similar to the plaintiff's registered trademark which, they alleged, had been registered only with the intention of earning illegal gains by commercially exploiting the same. The defendant however, argued that 'Tata Infotech' had been their trade name since 1997, and claimed to have earned a goodwill in the trade owing to a flourishing business. The court held that similarity in domain names could indeed result in diversion of traffic across websites, and could even cause economic loss to the registered right-holders of the original trademark

[9]Yahoo Inc. v Akash Arora (78(1999) DLT 285)
[10]Tata Sons Ltd. &Anr. v. Arno Palmen&Anr *2013(54) PTC 424 (Del)*

owing to the outreach of e-commerce and cyberspace. It was hence held that the impugned website had been registered with mala fide intentions in bad faith with the sole objective of acquiring advantage from exploitation of the plaintiff's registered trademark.

There are also instances called 'Reverse Domain Name Hijacking', wherein, parties come up with false allegations of cybersquatting against rightful owners through legal actions, as a result of which, such rightful owners end up transferring their rights to the fraudulent claimants for the sake of avoiding legal costs. Cases of reverse domain name hijacking hence has been seen to happen majorly against small entities or individual owners of trademark who often lack the financial strength to take up expenses involved in litigation.

1.6DISPUTE RESOLUTION IN CYBER LAW LEARNING OBJECTIVE

Resolution of disputes arising from use of cyberspace beings forth some basic problems which are critical to address. Owing to the global outreach of cyberspace, there often arise instances wherein the potential parties involved in a cyber dispute are residents of two different countries. Further complications arise when the dispute occurs in a territory which is different from the country of origin of either of the parties involved in the dispute. Such situations give rise to critical questions of jurisdiction which become difficult to resolve. Additionally, in cases where the disputes concern the technology and/or its rapid advancement, the law often fails to keep pace with such upgradations and succumbs to the gap which takes substantial time to be bridged. For example, by the time a court of law successfully passes a decision on a specific dispute, the technology might have become outdated and irrelevant.[11]

In an attempt to reduce the confusion, several jurisdictions have come up with their own territorial laws to tackle disputes relating to cyberspace wherein specific situations of jurisdictional issues are addressed to address cyber crimes. Additionally, principles of private international law gain relevance in the context of disputes arising from cyberspace, and have served as effective in establishing successfully resolution. Private International law being flexible and laden with doctrines and principles, situations causing cyber disputes are subjected to tests and

[11] Ethan Katsh and Janet Rifkin, Online Dispute Resolution: Resolving Conflicts in Cyberspace (Jossey-Bass, San Francisco, 2001) at 26 [Katsh and Rifkin].

approaches for analyzing which principle or doctrine would ideally apply. Furthermore, mechanisms of additional dispute resolution such as arbitration, mediation, negotiation, etc. often serves as effective in resolving disputes arising from use and exploitation of cyberspace.

The Judicial dispute resolution under Trademark Dilution Act and Anti Cybersquatting Prevention Act has been primarily performed by the US Courts, whereas non-judicial dispute resolution under UDRP has been done by following ICANN approved dispute-resolution service providers[12]:

- Asian Domain Name Dispute Resolution Centre (ADNDRC)
- CPR Institute for Dispute Resolution
- National Arbitration Forum
- World Intellectual Property Organization

In India, the Information Technology Act, 2000 attempts to address cybercrimes and disputes and provides for quasi-judicial bodies to be established for unencumbered dispute resolution. As per the provisions of the Act, adjudicating officers are to hear disputes of both civil and criminal nature relating to cyberspace and adjudge such cases to ward damages in civil remedies or impose penalties in case of criminal offences being committed. The Act further allows appeals being filed before the Cyber Appellate Tribunal and subsequently before the High Court address disputes involving cyber law.

1.7CONCLUSION

Over the last couple of decades, intellectual property has become assets owned by the right-holders. There is no denying the necessity of protecting intellectual property on or off cyberspace, for it acts as fuel for most modern trades. Owing to the exposure, outreach and enormity of cyberspace, content on the internet especially that including intellectual property requires all-round protection to restrict as well as remedy potential misuse. With the growth in technology, there is ever-increasing scope of new challenges emerging which might need advanced legal measures and stricter regulations for ensuring a balanced platform for all the interested parties

[12]eResolution [eRes] (approved effective 1 January, 2000; not accepting proceedings commenced after 30 November, 2001).

involved. Cyberspace needs to be bound by specific legal regulations today, more than ever.

1.8LET'S SUM UP

In this chapter, we have studied about the interface of cyber law with respect to copyright and trademark law along with case laws pertaining to it. In furtherance, we have also seen an overview about cybersquatting and the dispute resolution in cyber law.

1.9FURTHER READING

- Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publications, Edition 4th, 2011
- RohasNagpal, Intellectual Property Issues and Cyberspace, Asian School of Cyber Law Publication,Pune,2008
- S. K. Varma& Mittal, Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, 2003
- V.K. Ahuja, Intellectual Property Rights in India, Lexis Nexis Butterworth's Wadhwa, Nagpur, 2009

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. How does copyright law overlap with cyber laws?

Copyright law aims to foster creativity and innovation which the copyright owner and/or holder may subject to commercial exploitation. Cyberspace serves as the perfect medium for fulfilling such purposes. However, copyright law has suffered extensively as a result of exposure to emerging technologies by adversely affecting copyright owners through easy access of content and elimination of the distinction between private and public use so as to result in copyright infringement and the dilution of the grounds thereof. This is how cyberspace and cyber laws overlap share an interface with copyright laws.

2. How are trademarks and domain names related to cyber laws and cyberspace?

Domain names represent the IP address used in surfing the world wide web owing to which, the strictly territorial nature of trademarks has now broadened to become global. In the developing cyberspace, misappropriation of domain names not only cause immense damage to the business of infringed chain of goods/services, but

also destroys the goodwill associated with such brands completely. Cyber laws attempt to address such misappropriation.

3. What is cybersquatting?

Cybersquatting refers to the act of registering names of well-known companies and brands as domain names by fraudulent entities with the malafide intention of reselling the same elevated prices for making profits.

4. Describe the process of dispute resolution associated with cyber crimes and cyber laws?

Owing to the global outreach of cyberspace, individual jurisdictions have come up with their own territorial laws to tackle disputes relating to cyberspace wherein specific situations of jurisdictional issues are addressed to tackle cyber crimes. Additionally, principles of private international law also become relevant and serve as effective in arriving at successful resolutions. Furthermore, mechanisms of additional dispute resolution such as arbitration, mediation, negotiation etc. often serve to be effective in resolving disputes arising from the use and exploitation of cyberspace.

5. How does the Information Technology Act, 2000 address resolution of disputes associated with cyber crimes?

The Information Technology Act, 2000 attempts to address cybercrimes and disputes through quasi-judicial bodies to be established such dispute resolution. As per the provisions of the Act, adjudicating officers are to hear disputes of both civil and criminal nature relating to cyberspace and adjudge such cases to ward damages in civil remedies or impose penalties in case of criminal offences being committed. The Act further allows appeals being filed before the Cyber Appellate Tribunal and subsequently before the High Court address disputes involving cyber law.

1.11 ACTIVITY

Elaborate the Intellectual Property issues in cyber law? (1500-2000 words)

Unit 2: Usage of Internet and the Evolving Challenges of IPR Issues in India

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Present issue of IPR in India in light of Internet usage

2.4 Exploring the idea of liability

2.5 Internet and its impact

2.6 Let's sum up

2.7 Further reading

2.8 Check your progress: Possible Answers

2.9 Activity

2.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- To review the existing issue on IPR issues in India
- To study the existing IPR issues evolving from the unawareness of cyber laws.
- To evaluate whether increased usage of the internet shall create new IPR issues in India

2.2 INTRODUCTION

For an intellectual property right controller, the Internet presents two fundamental challenges: what to manage and how to administer. The increased usage of the Internet is expected to pose a greater threat to IPR security than it does now. While the Internet is poised to take off in the world, there are no realistic solutions to the intellectual property rights problems that it raises due to a scarcity of scientific expertise on the subject. There are already problems of intellectual property rights, but they are more theoretical than realistic.

The growing use of the internet carries with it concerns of intellectual property rights (IPR) security, which is critical in the current environment. Currently, the country is unfazed by the vast challenge of infrastructural growth required for Internet availability, and thus this requirement can be met in a matter of years. The internet can be accessed from anywhere in the world. Priority issues include the laying of high-speed national broadband networks and the provision of adequate telephone lines.[13]

To allow Internet services, a large number of nodes have been deployed in over two dozen cities across the world. The government has granted appropriate permission to private firms to make Internet services accessible in order to speed up the process of provision of this sophisticated and fast means of the communication network. India would become a major Internet consumer in the world as a result of the entry of private Internet service providers, much as it did in the cable television service market. The increased usage of the Internet is expected to pose a greater threat to

[13]Aggrawal, Artee& Trivedi, Jatin& Burman, Sucheta. (2015). Usage of Internet and the Evolving Challenges of IPR Issues in India: A Review. International Journal of Business Quantitative Economics and Applied Management research. 1. 1-10.

IPR security than it does now. While the Internet is poised to take off in the world, there are no realistic solutions to the intellectual property rights problems that it poses due to a lack of scientific expertise on the subject. There are already problems with intellectual property rights, but they are more theoretical than realistic.

The increased usage of the Internet is expected to pose a greater threat to IPR security than it does now. While the Internet is poised to take off in the world, there are no realistic solutions to the intellectual property rights problems that it raises due to a scarcity of scientific expertise on the subject. There are already problems with intellectual property rights, but they are more theoretical than realistic. This paper examines the current problems in the field of intellectual property rights that have arisen as a result of India's increased use of the internet.[14]

2.3PRESENT ISSUES OF IPR IN INDIA IN LIGHT OF INTERNET USAGE

Copyright law is currently the most important tool for dealing with IPR problems on the Internet. The Indian Copyright Act, which was first enacted in 1957. The Act has been amended five times since its enactment i.e., in 1983, 1984, 1992, 1994, 1999 and 2012. The Copyright (Amendment) Act, 2012 is the most substantial and in alignment with digital transformation in general ad internet in particular. The Copyright Act is now considered a piece of law, and the general outlook is that the revised Act will be able to withstand copyright problems arising from emerging technology, particularly those arising from the Internet. The Act has adapted to the modern age by dropping some limiting clauses and phrases and extending the meanings of works like cinematograph films (motion pictures) and sound recordings (phonograms) to allow certain works in "any format" within their purview. It does not, however, cover all facets of the digital problems that are now surfacing. Establishing the distinction between proprietary and public usage is one of the most significant copyright problems on the Internet. The Indian Copyright Act, like all copyright laws around the world, distinguishes between copying for public and private use.[15]

Reproduction for public use requires the consent of the right holder, while fair dealing for private use, study, critique, or evaluation is permissible by statute. With the

[14] Barlow, J. P. (1995). Property and speech: Who owns what you say in cyberspace?,Association for Computing Machinery.Communications of the ACM, 3(12), 19.

[15] Maloney, M. C. (1997). Intellectual property in cyberspace. The BusinessLawyer, 53(1), 225-249.

potential for an author to upload some copyrightable work to a large number of users concurrently over the Internet from the privacy of his or her house, and users being able to receive a perfect copy of the material sent simultaneously in their homes, this distinction becomes meaningless. Many people assume that a new generation of copyright norms is needed because the fine line between public and private lands is eroding. Another case in point is that of publishing.

Publishers of books and music have made their influence known since the arrival of the industrial revolution and the era of mass manufacturing. The value of their existence has grown to the point that authors cannot picture a future without them. The Internet has evolved into a powerful tool that has eliminated the middleman between a writer and his or her audience. An author's work is published on the Internet, and readers can access it directly. The Internet, by inspiring any writer to be a publisher, has once again served as an alarm bell, if not the death knell, for the publishing industry, which was born with the invention of the printing press.

This fact begs the question of whether making a job available on the Internet qualifies as a "publication." "Publication" for copyright purposes, according to the Indian Act, involves "making a work accessible to the public by issuing copies or communicating the work to the public." Because of its non-restrictive nature, this term can be interpreted as including electronic publishing and, as a result, "publication on the Internet." However, it will take a few years for electronic publication to make a significant impact in India. The fact that communicating over the Internet is "public contact" is still an open question. The Indian Act has a detailed description of the term "public contact." According to the Act, "communication to the public" requires "making any work accessible for public viewing, hearing, or enjoyment directly or through any means of presentation or diffusion other than issuing copies of such work, regardless of whether any member of the public necessarily sees, listens, or otherwise likes the work so made available."[16]

This description is sufficiently descriptive to include Internet-based communication within its framework. In view of this, Internet service providers in India would have a difficult time deciding who holds the rights to the Internet's content. Another issue is the proper distribution. The sales right in Indian law is also terminated after the first

[16] Tanenbaum, W. A. (1998). The challenge of cyberspace intellectual property.The Computer Lawyer, 15(2), 14-18. Features, Design, Photography, Technology,and Publishing Editors. (1998, Apr07.

delivery, as it is in most copyright laws. In the current situation, a student can sell a used textbook, and a library can distribute the books it has bought to its members.

Since no single copy can be circulated without duplication on the Internet, dissemination is limited to reproduction. On the Internet, the question of the right to reproduction raises a number of fundamental issues. This stems from the very essence of Internet transmission. Any stage of transmission requires replication. Temporary copying (also known as caching) is an essential aspect of the Internet communication mechanism through which messages will not be able to pass across the networks to reach their intended destinations. And if a user just needs to browse, transient copying occurs on the user's screen.

Coverage of temporary reproductions was a hotly contested subject at the World Intellectual Property Organization (WIPO) Diplomatic Conference in December 1996, but the outcome has remained ambiguous to this day. Can a reproduction be prohibited where it happens in the context of permitted use of the work and its primary objective is to make the work available, or when the reproduction is of a temporary or incidental nature? According to Indian law, reproduction must take the form of a tangible entity, but it also requires "storing it in any medium through electronic means." Case laws are yet to specify whether reproductions happening in Internet interactions are protected by the law's right of reproduction, and once that occurs, views on temporary and permanent reproduction, as well as the validity of temporary reproduction, can differ.

2.4EXPLORING THE IDEA OF LIABILITY

The problem of responsibility is one of the most critical facets of copyright compliance. There is also the matter of responsibility for actions performed during the delivery of a legitimate (as opposed to an infringed) copy of a work. As previously mentioned, the question is heavily contingent on the judiciary's understanding of different legal rights. When the court decides that in-transit copying, for example, is a breach of a patent, concerns about responsibility emerge. Who should be made accountable? Who is responsible for dispatching the job, receiving it, or the Internet service provider? The solution may not be quick to come by. Another factor is the transmission of a directly infringed copy of work over the Internet. The central argument, in this case, is whether an Internet service provider should be found liable for a subscriber's copyright violation even though he is ignorant of the subscriber's

behaviour. The Indian Copyright Act assumes that the infringement or abetment of the infringement must be done “knowingly” by an individual in order to be deemed a copyright violation. There is a reasonable risk that an Internet service provider, who may not be aware of the subscriber’s copyright violation, may be excluded from prosecution and penalty because of the term “knowingly.”[17]

However, the above factor poses a new concern. Even if the Internet service provider is not found guilty under Indian law, he may be found guilty under the laws of another region. How does one control the internet, which by its very existence, is universal and cannot be limited by national borders? Since the networks are widely distributed around the globe, a message or piece of information may be sent via a variety of countries before reaching its final destination.

The Internet service provider may not be liable in the country of origin or the country of destination, however, he or she may be liable in a transfer country. This is a problem that affects the whole world. The regulation of national IPR legislation bound by federal authorities in the seamless world of the Internet poses challenging problems. As a result, international law cooperation is urgently needed in this area; if this is not achieved, the possibility of litigation in some countries will force the Internet service provider to review the content being distributed for copyright approval, causing a pause in the whole procedure. The challenge is to speed up rather than slow down the flow of information. Any important technical innovation triggers a trend change, and the Internet is no different. Better norms must be established to delegate obligations to the parties involved; an Internet service provider is not always an enabler of copyright infringement.

2.5INTERNET AND ITS IMPACT

Finally, we should state that the Internet as a medium is extremely complex. It is also expected to be widely used in India, with the government announcing ambitious plans to make it available throughout the world. This is a challenge that the private sector providers have taken very seriously. As newer technology present more nuanced problems to a society, the widespread use of the internet will pose a

[17]Posch,RobertJ.,,Jr. (1999). Will intellectual property rights diminish incyberspace? Direct Marketing, 61(9), 29-31.

significant danger to the current copyright act. The protection of the rights of service providers, producers of generated content, and customers is a major challenge and mission.

We have a clear understanding that the Indian copyright act, as amended, is capable of dealing with the above issues to a large degree, but there is still room for progress in this field. The IPR administrator faces a unique difficulty in balancing the rights of various Internet actors such as content companies, security providers, access providers, and so on. This must be accomplished without jeopardizing the free exchange of knowledge while still guaranteeing that the legitimate economic rights of intellectual property creators are not jeopardized. The Internet's IPR privileges are reliant on this. The task for the IPR administrator is to determine how to implement the IPRs on the Internet in the most cost-effective way after they have been determined.

2.6LET'S SUM UP

In this chapter, we have learned the scope of IPR in light of internet usage. Besides, we have also analyzed the existing legal framework in the said area along with its interface with international conventions. We have also studied the concepts like-publication, communication etc, as per Indian legislations.

2.7FURTHER READING

- Barlow, J. P. (1995). Property and speech: Who owns what you say in cyberspace? Association for Computing Machinery. Communications of the ACM, 3(12), 19.
- Cohen, J. B. (1996). Dilemma in cyberspace. Editor & Publisher, 129(51), 20-21.
- Maloney, M. C. (1997). Intellectual property in cyberspace. The Business Lawyer, 53(1), 225-249.
- Tanenbaum, W. A. (1998). The challenge of cyberspace intellectual property. The Computer Lawyer, 15(2), 14-18. Features, Design, Photography, Technology, and Publishing Editors. (1998, Apr07.

- Cohen, J. E. (1998). Lochner in cyberspace: The new economic orthodoxy of “rights management”. Michigan Law Review, 97(2), 462-563.
- Posch,RobertJ.,,Jr. (1999). Will intellectual property rights diminish in cyberspace? Direct Marketing, 61(9), 29-31.
- Elsmore, M. J. (2000). The implications of intellectual property law for the auditing and protection of national and international brands: Part I. brands in cyberspace. Managerial Auditing Journal, 15(3), 116-132.

2.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is “publication”?

“Publication” for copyright purposes, according to the Indian Act, involves “making a work accessible to the public by issuing copies or communicating the work to the public.” Because of its non-restrictive existence, this term can be viewed as including electronic publishing and, as a result, “publication on the Internet.”

2. What do you mean by “communication to public”?

Whether or not any member of the public necessarily sees, receives, or otherwise likes the work so made possible, communication to the public involves making any work available for viewing, hearing, or enjoyment by the public directly or by any way of presentation or diffusion other than issuing copies of such work.”

2.9ACTIVITY

Elaborate upon the concept of liability in light of Intellectual property right and its related issues with internet usage. (Word count- 2000 to 2500)

Unit3:CYBERSPACE–CONFLICTING JURISDICTIONAL SPHERES OF IPR

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 What is Internet?

3.4 Jurisdiction in International law

3.5 Jurisdiction of copyright infringement on internet

3.6 Protection of copyright on Internet

3.7 Data protection on internet

3.8 Recent cases on internet jurisdiction

3.9 Let's sum up

3.10 Further reading

3.11 Check your progress: Possible Answers

3.12 Activity

3.1 LEARNING OBJECTIVE

In this chapter we will learn-

- How the traditional principles of jurisdiction are being adapted to amenability of jurisdiction of cyberspace-origin cases.
- About the existing IPR issues evolving from internet.
- About various provisions of law dealing with cyber related aspects.

3.2INTRODUCTION

Cyberspace is a technically amorphous vacuum, and its jurisdiction encompasses many fields of law and policy, including intellectual property rights violations, which is highly nuanced by copyright jurisprudence, and trade-related concerns. In cyberspace, IP security is divided into four categories: copyright, data protection, trademark, service mark, trade name, and trade dress, and domain names. In light of competing arguments that are litigated in a conventional manner without a particular model of jurisprudence suitable for settlement of various jurisdictional problems arising from technical advancement, the jurisdictional sphere of cyberspace assumes prominence. A single transaction in cyberspace can be governed by the laws of at least three jurisdictions: (1) the user's home state/nation, (2) the server hosting the transaction's home state/nation, and (3) the laws of the state/nation that refer to the individual or company with which the transaction is conducted.[18]

Jurisdiction corresponds to judicial, legislative, and administrative independence and is a legitimate component of state sovereignty. Despite the fact that authority is a part of sovereignty, it is not synonymous with it. The rules of a country which have extraterritorial effects, stretching the country's authority beyond its sovereign and temporal boundaries. This is especially concerning because the Internet is a tool that does not specifically recognize sovereignty or national boundaries. There is no universally applicable international jurisdictional rule, and certain issues are usually treated as matters of violation of laws or private international law. For example, a website's content can be legal in one country but illegal in another. Judicial

[18] Achieving legal and business order in cyberspace: A report on global jurisdiction issues created by the Internet, Business Lawyer, 55 (2000) 1801.

professionals are often faced with a conflict of law in the absence of a uniform jurisdictional code.

In the case of United States v. Jake Baker,[19] the defendant faced criminal prosecution for his online conduct, notwithstanding the fact that his case established a precedent for the right to free expression on the Internet. Furthermore, in the near past, a number of developers of peer-to-peer filesharing applications have been subjected to federal litigation for copyright violations. When these suits are international in scope, though, the scheme becomes incompatible. Simply put, what is lawful in one country can be unlawful in another. In reality, in a civil case, even separate requirements for the presumption of evidence will create jurisdictional squabbles. Actually, the authority is determined by the location and operation of online groups, which is based on the minimal touch principle. The vanishing point in copyright jurisprudence is cyberspace. The union between the virtual and physical worlds is a fertile ground for the birth of new theories and vast explorations that span all aspects of living things. The relentless revolution in knowledge flow and communication technology is forcing a worldwide rethinking of the concept of intellectual property legal regime. Infringement of intellectual property rights on the Internet has reached previously unheard-of levels. Standard forms of security such as copyrights, trademarks, licenses, applications, databases, and so on currently prove to be unable to address many of the issues, and no tailor-made alternatives seem to be on the horizon. This artistic illusion has impacted governments, companies, and people all over the world– particularly in a world where virtually every action is a copy, where creativity happens at a breakneck rate, and where knowledge is shared almost instantly and for free. These hydra-headed problems provide the developing world with the challenge of an incoming wave of structurally applied mechanisms, based on property rights and enforced by the world's most wealthy, intellectual property-exporting nations.

3.3WHAT IS INTERNET?

The Federal Networking Council (FNC) overwhelmingly passed a resolution describing the word Internet on October 24, 1995. It defines the Internet as a global

[19] US v Jake Baker, 890 F. Supp. 1375, 1381, 1997 Fed App. 0036P (6th Cir)

information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; and (ii) can support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IPcompatibleprotocals; and (iii) offers, utilizes, or renders available high-level services layered on the communications and associated infrastructure listed herein, whether publicly or privately.

Origin and Subject Matter of Disputes

Conflicts in cyberspace may have a variety of causes. One significant and recurrent source is an Internet arrangement. While a website connecting arrangement is an example of an Internet-only agreement, Internet agreements do not often mean Internet-only agreements and also have other elements.[20] A few of the forms, such as the celebrity endorsement deal, have just a shaky Internet connection. Terms of use arrangements, video content licensing agreements, domain name acquisition agreements, website creation agreements, press releases for website milestones or announcements, privacy policy, Internet advertisement agreements, copyright and patent rights notices, website disclaimers, website contracts, and more are among the legal documentation required for websites.

3.4JURISDICTION IN INTERNATIONAL LAW

In international law, there are three forms of jurisdiction that are commonly recognized. There are: (1) the power to prescribe; (2) the power to enforce; and (3) the power to adjudicate. The following are the types of historically recognized bases of authority or doctrines in which a state may assert jurisdiction to prescribe a rule of law over an operation in international law: Subjective territoriality (b) reflective territoriality (c) nationality (d) security principle (d) passive nationality and (e) universality, with the stipulation that authority must be exercised in a fair manner.[21] The territoriality issue in cyberspace can be resolved by pointing to the 'law of the site,' i.e. the server where the website is physically stored. If applied literally,

[20]Justice S. Muralidhar, Jurisdictional Issues in Cyberspace, THE INDIAN JOURNAL OF LAW AND TECHNOLOGY.

[21]Ms. Prevy Parekh, *Cyberspace And Jurisdiction*, JOURNAL ON CONTEMPORARY ISSUES OF LAW (JCIL) VOL. 2 ISSUE 5.

territorialization of cyberspace through its servers has a number of issues, including the existence of a webpage without its accessibility, constituents of a web page collected from other servers, links to other pages located in other countries, and the randomness and anonymity of cyberspace interactivity. The philosophy of foreign space, which includes outer space and the high seas, is based on nationality rather than territoriality. The relevant definition in outer space is the nationality of the vessel's registration, whether manned or unmanned, while on the high seas, the nationality of the vessel, or the "rules of the flag," is the predominant norm. A conflicting theory compares the high seas to a "floating island," with the jurisdiction falling under federal jurisdiction. Furthermore, the prevailing ideas of res nullius (a matter of no one) and res communis (a thing of all) confuse definitions of special significance in disagreements over international spaces (a common thing or common heritage of mankind).

3.5JURISDICTION IN COPYRIGHT INFRINGEMENT ON THE INTERNET

The following quote exemplifies how closely copyright and the Internet are linked: 'Since its inception, the Internet has been described as the biggest threat to copyright.' The Internet is awash in material, all of it protected by copyright to varying degrees. News stories, apps, books, screenplays, animations, videos, Usenet posts, and even email are examples of copyrighted works on the Internet. In truth, the frightening reality is that copyright law protects virtually everything on the Internet. That can cause issues for the unfortunate surfer'.[22]

3.6PROTECTION OF COPYRIGHT ON THE INTERNET

Electronic copyright is a modern phenomenon that is emerging, and with it comes a legal shift in the field. Copyright covers the originality, underlying architecture, and contents of a webpage, including links, original text, images, audio, video, html and other markup language sequences, lists of websites assembled by a person or entity, and any other special elements that make up the material's original existence. There are some inherent limits of copyright rights. Only original means of presenting facts and concepts are preserved. Fair usage makes up almost half of the copyright law, which gives you restricted ability to use other people's art without their

[22] The Copyright website, http://www.benedict.com (1 May 2010)

permission. Since terms like “fair” and “rational” are difficult to describe exactly, it is the least clear-cut copyright cap.

Films, tv programs, images, paintings, and artwork, including screenplays, teleplays, and blueprints, are all protected by copyright in the artistic domain. The main issue is combining all of the above without infringing on someone’s copyright with one or more of them. Many jurisdictions have a scheme for licensing internet works, which may or may not cover computer systems and automated databases, which have their own registration laws. Only the copyrightable content of the work identified as the subject of the copyright and deposited with the copyright office with appropriate application forms (US Circular 66) is protected. This includes literary works, visual art works, performing art works, sound recordings, serials and periodicals, and mask works, to name a few.

Apart from that, copyrights exist in software as well. The fundamental concept of English law, for example, is that the author of the code holds the copyright in the script or website. The fact that the individual commissioning the work has paid for it has no bearing on this. This law has two significant exceptions. To begin with, if the work was performed by a business employee, the copyright belongs to the boss. Second, the author has passed possession of the copyright by a signed contract that allows the author to delegate ownership to another person, typically the client.[23]

In spite of legal precedent, Religious Technology Centre v Netcom[24] and Playboy Enterprises v Frena[25], two American cases dealing with Internet copyright problems, did not include international jurisdictional issues. Both cases involved American citizens prosecuting other Americans, who were both explicitly subject to American territorial control.

3.7DATA PROTECTION ON INTERNET

Purchasing directories, security cameras, cell phone monitoring, wiretapping, manipulation of medical records, genetic profiling, and other practices have jeopardized anonymity, the most basic civil right. Since servers regularly record information about users’ e-mail and web surfing activities, Internet service providers

[23] Darrel C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, 4 Mich. Telecomm. & Tech. L. Rev 69, 72(1998)

[24] Religious Technology Center v Netcom, 907 F. Supp. 1367 (N.D. Cal 1995).

[25] Playboy Enterprises v Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

can provide a lot of information about them. The European Court of Justice (ECJ) handed down decisions in four cases in November 2004 concerning the interpretation of the EU Directive on the Legal Rights of Databases, which gives the maker of a database a sui generis database privilege (as opposed to copyright) where there has been a substantial investment in either the acquiring, verification or display of the database's contents.

Now GDPR is the new development with respect to data protection. The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA.

In India the Personal Data Protection (PDP) Bill, 2019 is the India's first attempt to domestically legislate on the issue of data protection.The Bill derives its inspiration from a previous draft version prepared by a committee headed by retired Justice B N Srikrishna.

3.8RECENT CASES ON INTERNET JURISDICTION

A French court[26] recently took control over Yahoo, an American internet news company, and ordered it to delete web sites containing Nazi memorabilia, which is illegal in France but legal nearly anywhere else. In a separate case[27], a British court found a British citizen responsible for sharing images on an American web server that were deemed indecent in the UK but not in the US.

In the case of **United States v Galaxy Sports**[28], an American court found the president of an Antigua-based gaming corporation responsible for soliciting and

[26] LICRA, French Union of Jewish Students v Yahoo Inc USA, Yahoo France, Tribunal de Grande Instance de Paris, Interim Court Order, November 2000.
[27] R v Waddon [2000] All ER (D) 502.
[28] United States v Galaxy Sports, US Department of Justice, (28 Feb 2000), http://www.usdoj.gov/criminal/cybercrime/ cohen.htm (8 March 2010).

taking bets from Americans over the Internet, notwithstanding the fact that this principle may be harmful to the principles of comity, sovereignty, and economic ties in the era of free trade. In the lack of a long-term solution to the hydra-headed problems arising from the integration of more and more gadgets into the cyber world, a temporary solution must be sought. The United States District Court for the District of Virginia recently found that it had “In rem Authority” over domain name registrants residing in other countries who were guilty of cyber squatting in Virginia. It was not a contentious situation. Summary judgment was given to the appellant, setting a high bar for the application of the US Anti-Cybersquatting Act and the authority of US courts over international cyber squatters. The claimants in this lawsuit, Atlas Copco AB and Atlas Copco North America LLC[29], were the owners of a registered trademark in the United States. Atlas Copco filed a complaint against the defendant’s domain names: Atlascopcoiran.com, Atlascaspian.com, Atlascaspian.net, Atlascaspian.org, Atlascaspian.biz, Atlascapianir.com, Atlascaspianiran.com, Atlascap1an.us, Atlascapian.cc, Atlascaspian.tv, and Atlas-caspian.com, alleging that the defendant’s domain names: Atlascopcoiran.com, AtlascaspianThese domain names’ registrants tended to be from Iran, Afghanistan, or India. Nonetheless, the domain name registries were based in Virginia and were subject to the jurisdiction of this Court. Long-arm authority was not activated because the registrants did not have adequate connections with the department. Citing Continental Airlines Inc v ContinentalAirlines.com[30], the Court reasoned that it had in rem authority over the defendants. The Anti-Cybersquatting Act has now been shown to have the tentacles to capture cyber squatters finding paradise in international jurisdictions, and this concept should be embraced and emulated by other countries as well.

3.9LET’S SUM UP

We learned an outline of some terminology and legal issues relating to cyberspace in this chapter, and it then goes on to address the four clusters, including copyright, data security, trademarks, and domain names, with a focus on how conventional jurisdictional rules are being extended to jurisdiction in cyberspace root cases.

3.10FURTHER READING

[29] Atlas Copco v AtlasCopcoiran.com, 533 F. Supp. 2d 610 (ED Va. 2008).
[30] Continental Airlines Inc v ContinentalAirlines.com, 390 F. Supp2d, 507 (E.D. Va. 2005).

- CompuServe Inc v Patterson, 89 F.3d 1257, 39 U.S.P.Q.2d (BNA) 1502 (6th Cir 1996).
- Zippo Manufacturing Co v Zippo Dot Com Inc, 952 F. Supp. 1119 (W.D. Pa. 1997).
- LG Berlin 97O193/96 (Nov. 20, 1996), aff'd, KG, 5U659/97 (March 25, 1997).
- Citigroup Inc v City Holding Co, 97 F. Supp. 2d 549 (S.D.N.Y. 2000).
- Mink v AAAA Dev LLC, 190 F.3d 333 (5th Cir. 1999).
- Bensusan Restaurant Corp v King, 937 F. Supp. 295 (S.D.N.Y. 1996).
- Tech Heads Inc v Desktop Serv 105 F. Supp. 2d 1142 (D. Or. 2000)

3.11CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is internet?

The Internet is a global information system that I is logically connected by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) can support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IPcompatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure.

2. What are the categories of jurisdiction in International law?

In international law, there are three forms of jurisdiction that are commonly recognized. There are: (1) the power to prescribe; (2) the power to enforce; and (3) the power to adjudicate.

3.12ACTIVITY

Provide a detailed account of International jurisdiction under cyber space with respect to Internet. Substantiate it will relevant case laws. (2000 to 2500 words)

Unit 4: CYBERSECURITY AND THE THEFT OF INTELLECTUAL PROPERTY ONLINE

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Protocols

4.4 Key documents

4.5 Current issues

4.6 Partnership and actions to combat cybercrime

4.7 Future outlook

4.8 Let's sum up

4.9 Further reading

4.10 Check your progress: Possible Answers

4.11 Activity

4.1 LEARNING OBJECTIVE

In this chapter we will learn-

- The strategies to ensure cyber security and its related aspects with IPR.
- The relevance of international measures to make safer cyber space.
- The steps needs to be taken in form of policy formation to protect intellectual rights.

4.2 INTRODUCTION

Digital globalization has exploded in recent years, linking millions of people through information and communication technology (ICTs). Borderless trade options are becoming more prevalent, which is usually a good thing. Increased adoption of ICTs, on the other hand, is linked to higher rates of cybercrime. According to the United Nations Office on Drugs and Crime (UNODC), the number of internet-connected computers will outnumber humans six to one by 2020. This hyper-connectivity would inevitably lead to higher rates of cyber crime, as well as a correlation between traditional crime and the digital world. It is difficult to assign a territorial authority to cybercrime because of the multinational existence of ICTs. In order to adequately counter cybercrime in regards to intellectual property, the international community must collaborate and cooperate.[31]

Intellectual property rights are “legal rights that cover innovations and/or discoveries arising from intellectual activity in the technological, science, literary, or artistic fields,” according to the International Telecommunication Union (ITU). Intellectual property rights encompass a wide range of topics, from sculpture, the Olympic Rings, and research on microorganisms. For a set amount of time, these rights normally grant the artist full use of their work.

Cybercrime is difficult to define since it is so context-dependent. According to the UNODC, the spectrum of computer-related actions of personal, financial, or intellectual advantage or damage is so vast that combining them into a single definite and encompassing word is difficult. Cybercrime can damage any kind of online

[31]Loza de Siles, Emile. (2015). Cybersecurity and Cybercrime: Intellectual Property and Innovation. American Bar Association / Landslide. 2015. 6. 10.2139/ssrn.2644365.

property, making it a major problem for businesses and governments alike. While it can be difficult to describe cybercrime, its effect is undeniable. Cybersecurity threats have resulted of a trillion-dollar industry in lost intellectual property due to imitation and pirated products. The method of determining the extent of cybercrime is extensive and complex. When attempting to detect, counteract, and defend against cybercrime, scale, motive, meaning, and jurisdiction must all be taken into account. Because despite the exponential advancement in technology, the international community is also grappling with the effects of cybercrime on global businesses and property holders.[32]

Theft of intellectual property costs billions of dollars to copyright holders and legal companies all over the world. Theft of intellectual property further threatens invention and ingenuity by discouraging copyright due to the pervasive existence of this illegal enterprise. It also puts consumers' health and welfare at risk by overwhelming the market with counterfeit pharmaceuticals. By leveraging financial benefits from counterfeit drugs, these activities help finance transnational organized crime networks. Aside from the direct consequences of intellectual property piracy, there are a slew of other problems to consider. These include the theft of personal identity and financial records, the reduction of commercial market advantages, reduced product or service viability, and the failure of a business attributable to counterfeit goods.[33] It also results in significant financial losses for victims after the reality. Intellectual property piracy has a long-term effect on businesses and states, owing to court fines, cybersecurity lawsuits, missed contracts, and public relations expenses.

The Special Event on Cybersecurity and Development was organized in 2011 by the Economic and Social Council, in collaboration with the United Nations Department of Economic and Social Affairs and the International Telecommunication Union. This panel discussion aimed to raise awareness of cybercrime at the foreign policy level, recognize best practices for fostering a cybersecurity community, and consider strategies for a global response to cybercrime. Cybercrime is multifaceted, and the cybersecurity panel recognized the value of cooperation among Member States, the

[32] See, e.g., The Estonia Model: Why a Free and Secure Internet Matters, WOODROW WILSON INT'L CENTER FOR SCHOLARS (Apr. 21, 2015), http://www.wilsoncenter.org/event/the-estonia-modelwhy-free-and-secure-internet-matters.

[33] See Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

private sector, civil society, and law enforcement to develop a holistic solution to the problem.

4.3PROTOCOLS

Any breakthrough in the world of innovation faces a variety of threats. The web is one such vulnerability that has engulfed the actual commercial centre and transformed it into a virtual one. In order to secure the corporate interest, it is important to establish a powerful property management and insurance instrument, bearing in mind the huge amount of business and commerce that takes place in cyberspace. Today, any company must develop a powerful and widespread IP management system and insurance protocol. The robotic world's constantly approaching threats will, therefore be able to be tested and contained.[34]

There could be important protocols for ensuring cybersecurity, which include the following –

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Empowering Open Standards
- Strengthening the Regulatory Framework
- Creating IT Security Mechanisms
- Securing E-administration Services
- Assuring Critical Information Infrastructure

4.4KEY DOCUMENTS

The Copyright Treaty of the World Intellectual Property Organization (WIPO) is the cornerstone text in terms of intellectual property rights (WCT). The first is that writers, musicians, and recording producers shall have the freedom to store their works in digital form. The owner's right to disseminate work digitally to the public through the

[34] See Cybersecurity: How to Keep You and Your Clients from Becoming Tomorrow's Headlines, A.B.A. (Aug. 1, 2015), http://www.americanbar.org/news/abanews/aba-newsarchives/2015/08/cybersecurity_howt.html; Matthew Goldstein, Citigroup Report Chides Law Firms for Silence on Hackings, N.Y. TIMES, Mar. 26, 2015, http://www.nytimes.com/2015/03/27/business/dealbook/citigroup-report-chides-law-firms-for-silence-onhackings.html?_r=0 (discussing internal April 2015 report by Citigroup's Cyber Intelligence Center).

internet is the second concept. The third step is to use appropriate legal remedies to shield these multimedia works against unauthorized copying, sharing, or selling. The WIPO's Performances and Phonograms Treaty also acts as an outline of how to compose an intellectual property document for an emerging medium and how to deal with the interests of interactive media beneficiaries.

The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications (GGE) is a UN-mandated working group that has contributed to the development of the global cybersecurity agenda and adopted the concept of international law applying in digital contexts. Each meeting is followed by the development of a consensus paper, which has been lauded for its diversity of views, advice, and coverage of contentious topics. The group's recommendations for confidence-building interventions, capacity-building efforts, and infrastructure security are included in each study. Although the GGE's membership is comparatively limited, the association has made considerable strides in developing international cybercrime and cyber security norms.

The ITU convened the World Summit on the Information Society (WSIS) to facilitate equal access to the benefits of ICTs, such as e-commerce, e-governance, e-health, education, economic growth, diversity, and environmental conservation. The Geneva Declaration of Principles and Geneva Plan of Action from WSIS' first and second phases, respectively, the Geneva Declaration of Principles and Geneva Plan of Action from 2003 and the Tunis Commitment and Tunis Agenda for the Information Society from 2005, place a strong emphasis on growth, capacity-building, openness, and confidence-building steps to increase access to ICTs and cybersecurity.[35]

The Geneva documents are foundational documents that set out the international community's priorities, challenges, and objectives. The Tunis papers are more actionable in general, as they include detailed strategies for carrying out the obligations outlined in the Geneva Declaration of Principles and Plan of Work. The Council of Europe's Convention on Cybercrime is a valuable regional paper on cybercrime and its prevention. This is the first multinational treaty dealing specifically with cybercrime. It specifically addresses patent theft, computer-related fraud, and network protection breaches. The key goal of this convention is to pursue a universal

[35] Cyber Crime: Modernizing Our Legal Framework for the Information Age, Hearing Before the Subcomm. on Crime & Terrorism, of the S. Comm. on the Judiciary, 114th Cong. 3 (2015) (statement of David M. Bitkower, Deputy Assistant Att'y Gen., Criminal Div., Dep't of Justice), http://www.justice.gov/opa/file/627486/download

crime reduction strategy aimed at preventing cybercrime, especially through the adoption of relevant legislation and the promotion of international cooperation.

4.5CURRENT ISSUES

While the international community has many means to fight cybercrime, there are few manuals and instruments to direct their acts. Currently, the proposed international system for cybercrime in relation to intellectual property legislation is used in the broader definition of cybersecurity. The ITU is a member of the International Multilateral Partnership Against Cyber Threats (IMPACT), which is the world's biggest cybersecurity coalition. It's a networking forum for sharing cybersecurity best practices. IMPACT and the ITU collaborate to bring together the expertise of government, academics, business executives, and individuals to ensure global cybersecurity.The ITU has charged IMPACT with providing Member States with access to cyber threat experience, services, and infrastructure. It also aids UN organisations in safeguarding their information technology resources.

- ***Challenges of promoting cybersecurity***

Because of the complexities of cybersecurity, the international community faces many obstacles in combating cybercrime in relation to intellectual property rights. There are several issues that the international community as a whole must solve, as well as issues that Member States face on an individual basis. When a cybercrime happens, determining the magnitude of the damage is virtually impossible. This is attributed to a scarcity of accurate data and the absence of mechanisms to collect it. The fact that this is a transnational problem adds to the difficulty of solving such crimes. Huge economic inequalities exist between developing and developed nations, making it difficult for them to catch up with their advanced equivalents. Developing countries also lack the resources to fight cybercrime.

Since developed countries have little detection systems, they may become "safe havens" for cyber criminals. The lack of collaboration and collaboration between developed and developing countries exacerbates the problem. The ITU has created a guide for developed countries called Understanding Cybercrime: A Guide for Developing Countries in order to assist in tackling the issues that the international community is facing. Legislation, strengthened law enforcement, capacity building,

and preparation are some of the national and multilateral solutions to such problems. Such policies, on the other hand, cannot be implemented without adequate crime prevention and criminal justice programs, as well as the human capacity, financial, and technological tools needed to tackle cybercrime. Member States seeking assistance in areas such as access to ICTs and establishing better cybersecurity are supported by the ITU. - case is treated independently and begins with a review of the country's current ICT situation. The ITU will then include a customized guide to help the Member State achieve its ICT objectives. These roadmaps tailor capacity-building plans and provide guidance on policies that can be used to improve cybersecurity.[36]

4.6PARTNERSHIPS AND ACTION TO COMBAT CYBERCRIME

A lot of work has been done on this subject in the private sector and in academia. In addition, private sector organisations see cybercrime involving intellectual property as a larger concern than Member States. There is now a wide movement within academia to not only consider cybercrime phenomena, but also to create effective technologies to fight them. Non-profit organisations such as the Knowledge Technology-Information Exchange and Analysis Center, which aims to improve cybersecurity for businesses by fostering cooperation, intelligence sharing, and incident management, are now helping to tackle cybercrime.

This not only helps the private sector escape intellectual property piracy, but it also allows various actors to learn and exchange best practices, preventing potential abuse by both parties, public and private. Public-private partnerships are also essential in the development of cybersecurity strategies. These collaborations are critical for fostering cybersecurity and development, particularly in developing countries. Private businesses frequently have the capacity and capabilities to more efficiently fight cybercrime while also fostering benefits in the host country, such as economic growth and human resource development.

[36] Nakashima, Ellen et. al. “Report: Cybercrime and espionage costs $445 billion annually.” The Washington Post. June 9, 2014. https://www.washingtonpost.com/world/nationalsecurity/report-cybercrime-and-espionage-costs-445-billionannually/2014/06/08/8995291c-ecce-11e3-9f5c9075d5508f0a_story.html?utm_term=.2d356b0ec666.

Cybercrime against intellectual property is considered a piracy problem by the International Police Organization (INTERPOL). Counterfeiting, piracy, and smuggling for tax avoidance are all considered illegal merchandise trafficking. As a result, INTERPOL will use all of its anti-trafficking capabilities to track down, interrupt, and shut down these activities. Supporting regional and global activities, capacity development and preparation, raising awareness, and offering legal assistance to Member States on request are INTERPOL's key activities against intellectual property cybercrime.[37]

4.7FUTURE OUTLOOK

On a global scale, there have been several debates about the implementation of an international conference on cybersecurity. In a perfect world, this convention will aim to harmonize national rules on cybercrime, such as copyright theft, hacking, and network security breaches. In order to promote the existence of binding treaties and further guidance, the GGE has also suggested the formation of a successor group.[38] The treaty will also support and reinforce efforts to fight cybercrime more quickly and efficiently than in previous years. Given the complexities of cybercrime and ICTs, however, such a treaty would almost certainly be complicated and take careful thinking and consideration. Professional assistance promotion, facilitation, and funding will further enhance those efforts, meaning that all Member States have the tools they need to mitigate the effect of cybercrime on intellectual property security.

4.8LET'S SUM UP

In this chapter, we have learned the possible steps, which can be taken to manage cyber security. Additionally, we have also analyzed the responsibility of international organisations and governmental institutions in ensuring cyber security and its aspects related to intellectual property rights.

[37]Passman, Pamela. "How to Protect Intellectual Property: from Fair Trade to Legal Trade." Foreign Affairs. February 27, 2013. https://www.foreignaffairs.com/articles/2013-02-27/howprotect-intellectual-property.
[38] "The Information Technology – Information Sharing and Analysis Center." IT-ISAC. July 16, 2017. https://www.it-isac.org/.

4.9FURTHER READING

- Taubman, A. (2009), 'International Governance and the Internet', in: L. Edwards and Ch. Waelde (eds), Law and the Internet, 3rd ed, Oxford and Portland, Oregon: Hart Publishing, pp. 3-44
- Torremans, Paul (2005), 'Authorship, ownership of right and works created by employees: which law applies?', 27(6) European Intellectual Property Review, 220- 224
- Vivant, Michel and Bruguière, Jean-Michel (2012), Droit d'auteur, 2nd ed., Paris: Dalloz
- Wilson, Caroline (2009), 'Domain Names and Trade Marks: An Uncomfortable Interrelationship', in: L. Edwards and Ch. Waelde (eds), Law and the Internet, 3rd ed, Oxford and Portland, Oregon: Hart Publishing, pp. 311-333.
- Rahmatian, Andreas (2009), 'Dealing with rights in copyright-protected works: assignments and licences', in: E. Derclaye, Research Handbook on the Future of EU Copyright, Cheltenham: Edward Elgar, pp. 286-316
- Rahmatian, Andreas (2011), Copyright and Creativity. The Making of Property Rights in Creative Works, Cheltenham: Edward Elgar

4.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Define Cybercrime

Cybercrime is difficult to define since it is so context-dependent. According to the UNODC, the spectrum of computer-related actions of personal, financial, or intellectual advantage or damage is so vast that combining them into a single definite and encompassing word is difficult. Cybercrime can damage any kind of online property, making it a major problem for businesses and governments alike. While it can be difficult to describe cybercrime, its effect is undeniable.

2. What could be possible protocol to ensure cuyber security?

There could be important protocols for ensuring cybersecurity, which include the following –

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Empowering Open Standards

- Strengthening the Regulatory Framework
- The Creating IT Security Mechanisms
- Securing E-administration Services
- Assuring Critical Information Infrastructure

4.11 ACTIVITY

In what ways might cybersecurity attacks on protected IP impact your Member State's social and economic landscape? (Word count- 2000 to 2500)

Block-2

COPYRIGHT AND CYBER LAW

1

Unit 1: COPYRIGHT IN CYBERSPACE

Unit Structure

1.1 Learning Objectives
1.2 Introduction
1.3 Copyright and its treatment in cyber space
1.4 Peer to Peer file sharing
1.5 Internet Service Provider Liability
1.6 Let's sum up
1.7 Further reading
1.8 Check your progress: Possible Answers
1.9 Activity

1.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- The relationship between copyright and internet.
- The concepts of downloading, Peer-to-Peer sharing and other related aspects of copyrights on cyber space.
- Various legal provisions governing copyright on internet.

1.2INTRODUCTION

Intellectual property rights are critical to the country's socio-economic and cultural growth. The evolution of the internet is humankind's greatest scientific accomplishment. The internet's unique capability to share insights, thoughts, and material in the form of images, graphs, and videos to any corner of the world in the same content in a fraction of a second. Infringement is on the rise as the usage of internet IPR grows. Linking, deep linking, uploading-downloading, copy-paste, and P2P file-sharing applications, which are often found on the internet, all require copyright problems. Protecting copyright in cyberspace is a huge problem for us because our copyright legislation, the Information Technology Act, does not relate to the changing new world because it is impossible to track down criminals in cyberspace due to the internet's extraterritorial authority. India is a signatory to the WIPO Internet Treaty, and the Copyright Act was amended in 2002 and 2012 to address internet concerns in order to satisfy international requirements. This provision, however, was insufficient to address the question of copyright rights in cyberspace. Copyright infringement poses a significant danger to all industrial sectors, including copyright, electronics, music, and the film industry, among others, and has a negative impact not only on owners' rights but also on the nation's economy. As a result, it is vital to fight internet piracy by maintaining effective copyright rights in cyberspace, which would automatically stimulate mankind's innovation. Around the same time, general knowledge and information about copyright are critical.

Patents, trademarks, architectural design, copyright, and proprietary documents all fall under the umbrella of intellectual property, which is a globally recognized

principle. Copyright is a crucial right in all forms of intellectual property protection because it prevents the illegal copying of original work. In the twenty-first century, the invention of new media has brought about fundamental improvements. Because of its attributes such as storing power, speed, intercreativity, interconnection, and operation beyond territorial boundaries, the internet presents many opportunities and challenges for copyright enforcement in cyberspace. It is very possible in cyberspace to take material from one platform and change and replicate it on another without revealing one's identity. Copyright Act, 1957 is revised from time to time for the defence of copyright, the most recent change being in 2012 to satisfy national and international specifications. While the Information Technology Act of 2002 exists, these statutes are unable to preserve copyright in cyberspace.

1.3COPYRIGHT AND ITS TREATMENT IN CYBER SPACE

Copyright is similar to other property rights, such as title, in that the landowner owns everything on the land, from the sky to the grass. Copyright works on the same concept but with certain restrictions.[39] Copyright compliance in cyberspace is hampered by the use of computers, the internet, and streaming, copying, copy-cut-paste, deep linking, and peer-to-peer file sharing. The following are the problems posed in defence of copyright in cyberspace:

Uploading & Downloading

Copyright infringement occurs when someone uploads proprietary works without permission. The standard of illegally downloaded songs, videos, and video games is bad, and it is punishable under India's Copyright Act. Even if he has not earned any financial benefit, the individual who posted the content is responsible. When an uploader uses his imagination to update, modify, or amend copyrighted content, he assumes responsibility. Illegal downloading is most common in the film, recording, music, gaming, and software industries. Piracy is a major issue in India's media and film industries, with copyright piracy costing the country $4 billion per year. Only when a user prejudicially distributes, exhibits or lets for selling or employ copyrighted content without sufficient consent commits an offence, according to Justice Gautam Patel of the Bombay High Court.

[39] http://nopr.niscair.res.in(Journal of Intellectual Property Rights,Vol.19,Sep.2014,pp307,Exploring Sovereign Immunity in Copyright Infringement:How India can learn from the Global Experience)

Linking

The world today is a worldwide web. The website provides a vast volume of material in the form of sentences, images, illustrations, audio, and other media. As a result, the copyright statute covers the website. The site's primary focus is on the electronic publication of this content. Designing or creating a website necessitates a significant amount of talent, labour, time, resources, and mental effort. As a result, preserving the website's intellectual property is important. Linking allows people to easily switch from one place to another and view information in a limited amount of time. It informs people about the life of work by including a clear website address. Linking is a feature that allows you to visit a third-party website by clicking on a location on the linking site without having to enter any location information or using a search engine.[40] Links are normally outlined, underlined, or conspicuous text or images. There are two ways of linking[41]:

1. Surface linking: Surface linking happens when a site's home page is linked.

2. Deep linking: Deep linking is where a connection skips the home page and goes directly to an internal page inside a favourite website. Only in regard to 'Deep connecting' do legal questions emerge, as this technology aids in the distribution of other people's artistic content. Copyright infringement is described as reproducing, issuing, or transmitting work to the public without authorization or consent, according to Sec.14,51. Deep linking sites are not specifically responsible for infringement since the duplication of work is performed by the individual who visits the linked website by the connection, not by the linking site.

Having any job available for the public to view, read, or enjoy directly or by any means of showing is considered contact to the public under Sec.2(ff). The Copyright Act does not expressly prohibit deep linking, but the phrase "by any means of view," as defined in Sec. 2(ff), includes sharing of a web site's contents over the internet. Communication of work without consent is considered copyright infringement under Section 51. It means that deep linking without the owner's consent is a kind of copyright infringement. Contributory Copyright Infringement happens when someone makes a link that is likely to facilitate unauthorized copying of copyrighted content,

[40]Lw relating to computers Internet & E-commerce,Universla Law Publishing Co.New Delhi-India,AuthorNandan Kamat,pp197

[41] Legal Dimensions of Cyberspace,Edited by S.K.Verma& Raman Mittal,Indian Law Institute,New Delhi,pp-119.

and the person that created the link has cause to know about the unauthorized copying.[42] Some websites, such as Amazon.com, welcome linking or deep linking because it enhances traffic, advertisement prices, and sales.[43]

Linking, also known as deep linking, is a technique for gaining easy access to information. Bixee.com, without the consent of Naukari.com, allowed users to access these jobs directly on its website, bypassing Naukari.com's home page, resulting in financial losses for Naukari.com. On the grounds of copyright violation, an Indian court barred Bixee.com from deep-linking, copying, uploading, and reproducing material from Naukri.com's website. In a nutshell, deep linking without authority entails the electronic publishing of information, copying, and contact to the public without consent, all of which constitute copyright infringement.

1.4PEER TO PEER (P2P) FILE SHARING

In general, file sharing refers to the electronic sharing of multimedia media (music, audio recordings, movies, tv shows, games, and computer applications, for example). Peer-to-peer (P2P) is a means of sharing files without the use of a middleman server. P2P technology was not intended to make copyright piracy simpler, but it is now being used to distribute unlawfully copyrighted content. Some P2P technologies, such as Napster, Gnutella, and Kazaa, are well-known and enable users to share, distribute, and update files across the internet without sacrificing efficiency. MP3 technology entails compressing sound recordings to a tiny size and distributing them over the internet in a limited period of time. The growth of MP3 necessitated the creation of a mechanism for transferring files over the internet, which led to the creation of Napster.[44] Only music files, especially mp3 files, were associated with Napster. Following the installation of the Napster program, you were directly linked to Napster's central server, which only included a list of music files accessible on Napster members' computers.

Simply type the name of an album or an artist to get a list of what's available, and then stream music from another user's machine who is online in a matter of seconds. As a secondary infringer, the court ordered Napster to cease distributing stolen

[42] http://smallbusiness.findlaw.com

[43] Legal Dimensions of Cyberspace,Edited by S.K.Verma& Raman Mittal,Indian Law Institute,New Delhi,pp-119.

[44] 1P2PNetworks : Online Piracy of Music,Films& Computer Software,Journal of Intellectual Property Rights,Vol9,Sep.2004,pp442 ,Author-Raman Mittal (Keith Taylor,Piracy in Cyber space: The battle over digital music on internet,http://guslaw.gus.edu/lawand/papers/fa02/taylor)

music and close down its website. In India, anybody operating a network similar to Napster is liable under Sections 14 and 51(a)(ii) of the Copyright Act, 1957. It resulted in the collapse of Napster and the rise of stronger peer-to-peer networks. Every individual who permits any location to be used for the transmission of the work to the public where such communication constitutes an infringement is liable for copyright infringement, according to Sec.51(a)(ii). The word “any place” includes both physical and virtual places.[45] Infringement occurs as someone makes copies of a work or communicates the same work to the public, according to Sec.14.

In the case of Napster in India, someone who downloads and installs the program is making copyrighted work accessible to any member of the community who has the software installed on his computer. It suggests that Napster is promoting online contact and that transmitting proprietary content to the public is infringing under Sec. 14. The person who copies a patented work file is reproducing the work without the permission of the copyright owner. As a result, he has committed patent theft. P2P technology, in short, poses a challenge to the copyright industry, which includes the music, sound capture, and software industries, because it allows for the copying and sharing of copyrighted works over the internet.

1.5INTERNET SERVICE PROVIDER LIABILITY (ISP)

When we first began using the internet, the issue of ISP responsibility for copyright infringement emerged. ISPs are businesses or organizations that allow clients to link to the internet. In India, ISPs such as Airtel, Idea, and Telenor offer internet connections and other connectivity services to users. Any concerns have been raised about ISP responsibility for copyright violations, such as whether ISPs are held responsible for criminal acts committed by their users. And to what degree was it found to be infringing? Usually, copyright owners sue ISPs for enforcing their copyright because ISPs are more financially capable of paying fines than actual private users, and that has a deterrent impact on holding ISPs responsible. When a website has several users who are all allowed to upload or download content to and from that website, if you take action against one of them, another user can infringe the following day. However, if you take legal action against the ISP, you can uninstall

[45] Legal Dimension of Cyberspace,Edited by S.K.Verma& Raman Mittal,Indian Law Institute,New Delhi,pp142

proprietary content from the website and advise their subscribers not to post illegal content. So, since the ISP dominates the network, it is very straightforward to protect copyright piracy by suing him personally.[46]

Different laws apply to ISP liabilities, including penal law, tort law, patent law, trademark law, and unfair competition law. There is no clause of the Copyright Act of 1957 that addresses the question of ISP liability. Sec.51(a)(ii) states that whenever any person permits for profit any place to be used for the transmission of work to the public where such communication constitutes an infringement of copyright unless he was not aware and has no reason to suspect that such communication would constitute an infringement of copyright.

Since computer servers and telecommunication facilities fall under ISP, which is a dimension of cyberspace, the term "every location" includes cyberspace, which contains ISP. So, under Sec. 51(a), 'any position' includes ISP (ii). Another phrase is "permits for profit," which means that ISP profited financially from infringing practices. So, if ISPs bill for their services and others are free, they are indirectly profiting from advertisements. It ensures that by distributing or holding infringing content, the above conditions of "permits for benefit" are met. Another condition is that they should only be held responsible if they have knowledge that the content processed or sent from their repositories is violating. If ISP satisfies all of the aforementioned criteria, it is presumed that he is infringing on someone else's copyright.

The Information Technology (IT) Act of 2000 contains rules on ISP liability. An intermediary is specified in Sec. 79(a) of the IT Act as any person who receives, stores, or transmits a message on behalf of another person or provides any service related to that message. The Internet Service Provider (ISP) is a form of intermediary. This provision, once again, restricts ISP's responsibility under some cases. According to this clause, an intermediary, such as a network service company, is not responsible whether he may demonstrate that the crime or contravention was done without his knowledge or that he used any fair attempts to avoid it. Practically, ISPs perform a variety of roles in the delivery of material, and their responsibility varies based on the sort of work they perform; otherwise, they would be kept responsible for information for which they have no control or over which they have never played any part. However, no statutes, including the

[46] 4 Legal Dimension of Cyberspace,Edited by S.K.Verma& Raman Mittal,Indian Law Institute,New Delhi,pp152.

Copyright Act, have been amended to restrict the liability of ISPs. The IT Act only allows ISPs to be found responsible for copyright violations if they offer filtering services.

1.6LET'S SUM UP

In this chapter, we have learned the overview of some terms and legal aspects related to cyberspace and copyright. Besides, we also learned various concepts revolving around internet sharing, downloading, internet service provider liability etc. We have also analyzed various legal provisions governing copyrights.

1.7FURTHER READING

- Jonathan Franklin, "Intellectual Property Law," Electronic Resource Guide, American Society of International Law, last updated February 8, 2013, accessed on August 2, 2013, http://www.asil.org/erg/?page=iipl#id.juy3tsp3onkv.
- Richard L. Hermann, Landing a Federal Legal Job: Finding Success in the U.S. Government Job Market (Chicago: American Bar Association, 2011), 277.
- Berkman Center for Internet and Society at Harvard University, "Overview of Trademark Law," accessed on August 2, 2013, http://cyber.law.harvard.edu/metaschool/fisher/domain/tm.htm.
- Library of Congress, The Congressional Research Service: www.loc.gov/crsinfo/

1.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is "any place"?

Since computer servers and telecommunication facilities fall under ISP, which is a dimension of cyberspace, the term "every location" includes cyberspace, which contains ISP. So, under Sec. 51(a)(ii) 'any place' includes ISP.

2. Explain "permit for profit".

The term “permits for-profit” refers to the fact that ISP profited financially from infringing practices. So, if ISPs bill for their services and others are free, they are indirectly profiting from advertisements. It ensures that by distributing or holding infringing content, the above conditions of “permits for benefit” are met.

1.9ACTIVITY

Explain Internet Service Provider Liability with relevant provisions of law. (2000 to 2500 words)

2

Unit 2: COPYRIGHT AND INFRINGEMENT IN CYBERSPACE

Unit Structure

2.1 Learning Objectives

2.2. Introduction to Copyright Issues in Cyberspace

2.3. Online Copyright Violation

- 2.3.1. Caching
- 2.3.2. Plagiarism
- 2.3.3. Protection of database
- 2.3.4. Protection of computer software

2.4. Computer software and copyright law

2.5. Software licenses

- 2.5.1. Freeware licenses
- 2.5.2. Open source Licenses
- 2.5.3. Shareware
- 2.5.4. Demo ware

2.6. Let's Sum up

2.7. Further Reading

2.8. Check your progress: Possible Answers

2.9. Activity

2.1 LEARNING OBJECTIVE

In this chapter, we shall be learning about-

- Various forms of copyright infringement in cyber space.
- Software protection and copyright laws
- Various forms of licensing.

2.2 INTRODUCTION TO COPYRIGHT ISSUES IN CYBERSPACE

The copyright's aim is to inspire writers, composers, and directors to create original works by giving them the exclusive right to print and publish them for the public good. When the limited privilege, i.e., the copyright term, expires, the works become public domain, and anybody can copy them without permission. Initial literature, tragic, theatrical, creative, cinematographic video, sound recording, and computer program are all protected by copyright.[47] Today, copyright is used in a wide range of sectors, including the publishing and sale of books, magazines, and newspapers, the manufacture and distribution of dramatic and artistic works for performances, the printing of musical works and cinema, broadcasting, and so on. Copyrights, as Intellectual Property, move more freely and rapidly from country to country than other types of property. Copying copyright content has become much simpler due to technical advances. As a result, copyright piracy has been difficult, if not impossible, to regulate. Books, recorded tapes, video cassettes of videos, and electronic programs can all be easily transported from one country to another, and thousands of copies can be manufactured and distributed. Unauthorized home recordings of radio and television programs have become popular around the world.[48]

Digital media has made it possible to take material from one site, change it, or simply reproduce it on another site, posing new problems for conventional interpretations of individual rights and security. A publisher can be anybody with a PC (Personal Computer) and a modem. It just takes a few mouse clicks to download, import, save, convert, or create a derivative work. Since it includes text, images, and also audio and video, a web page is equivalent to a print, a magazine, or a digital CD-ROM and

[47] Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publication, New Delhi, 2012, pg.no.28.
[48] Available at www.wipo.int , visited on 15/02/2016.

would be liable for copyright protection. The creator of a copyrighted work has the sole right to permit copying, preparation of derivative works, dissemination, and other activities under copyright law.[49]

2.3ONLINE COPYRIGHT VIOLATION

2.3.1 Caching:

Determining the distinction between private and public use is one of the most fundamental copyright problems on the internet. The Indian Copyright Act, 1957 distinguishes between reproductions for general use and reproductions that can only be achieved with the consent of the right holder. On the internet, the freedom to copy poses a variety of constitutional questions. Because of the fundamental essence of internet transmission, this is the case. Any stage of transmission involves reproduction. Temporary copying (also known as caching) is an essential aspect of the internet communication mechanism through which messages will not be able to pass across the networks to reach their intended destinations. According to Indian law, copying must be in a tangible way, but it also requires "storing it in every format through electronic means," making caching a copyright violation.

2.3.2 Plagiarism:

Copying copyright content has become much easier, thanks to technological advancements. As a result, copyright piracy has been difficult, if not impossible, to regulate. It entails using someone else's work without giving them credit, even though it were one's own original work. It is regarded as an ethical violation that may jeopardize one's intellectual standing and honesty. Plagiarism is possible without infringing on another's copyright, and infringing on another's copyright is possible without plagiarizing. Plagiarism and copyright violations can all occur at the same time. Books, videos, films, and music can all be easily replicated, and thousands of copies can be made and circulated. Digital media has made it possible to copy material from one platform, change it, or literally replicate it. The standard view of human rights and security under the Copyright Act has been thrown into disarray as a result of this.

2.3.3 Protection of Database:

The Indian Copyright Act 1957 protects "Databases" as "Literary Works" under Section 13(1) (a) of the Act, which specifies that copyright in original literary,

[49]V.K. Ahuja, Intellectual Property Rights in India, Lexis Nexis Butterworth's Wadhwa, Nagpur, 2009,at page nos.15-16

theatrical, musical, and artistic works shall exist in India. For the first time, the word "computer database" was established in the Information Technology Act of 2000. An individual who breaches the copyright and cyberspace norms is liable to pay compensation to the aggrieved party up to one crore rupees under Section 43 of the I.T. Act 2000. In addition, Section 66 of the Income Tax Act of 2000 imposes criminal penalties in certain cases.

2.3.4 Protection of computer software:

A computer programme is described as a "collection of instructions transmitted in words, codes, schemes, or some other type, including a machine readable media, capable of causing a computer to perform a particular task or achieving a particular result," according to section 2(ffc) of the Copyright Act. Within the scope of the Copyright Act, computer software is a "computer application." Computer programs now count for copyright protection, as well as other forms of Intellectual Property Rights protection, under the T.R.I.P.S (Trade-Related Aspects of Intellectual Property Rights). This programming programs are also covered by the Copyright Act's copyright protection. Under the Copyright Act, computer programs are included in the scope of literary content.

The owner of computer software has a variety of rights, including the ability to issue software licenses. Freeware licenses, open-source licenses, demoware licenses, and other forms of software licenses exist. The owner of a software patent has the freedom to reuse and render as many copies of his work as he wants. Second, he has the possibility of showing his program on the website, which will be called public view. He also has the rights to sell, rent, move, update, and change his proprietary software. Without the owner's consent, no one can use a copyrighted work for personal gain.

However, copyright infringement happens when someone uses a patented work for a commercial reason or to rob the author of income. Despite the fact that the software copyright owner has certain proprietary rights, they are not absolute and are subject to certain restrictions and exceptions in order to protect and preserve the public interest, including that of software users.

In certain socially desirable circumstances, such as literary, dramatic, musical, or artistic work for private use, including study, criticism, or review, the use of the copyrighted work is allowed even without the author's permission in order to use the computer program for the purpose for which it was supplied or to make back-up

copies purely as temporary protection against loss, destruction or damage in order only to utilize the computer program for the purpose for which it was supplied.

2.4COMPUTER SOFTWARE & COPYRIGHT LAW

A computer programme is described as a “collection of instructions transmitted in words, codes, schemes, or some other type, including a machine-readable media, capable of causing a computer to perform a particular task or achieving a particular result,” according to section 2(ffc) of the Copyright Act. Within the scope of the Copyright Act, computer software is a “computer application.” These programming programs are also covered by the Copyright Act’s copyright protection. Under the Copyright Act, computer programs are included in the scope of literary content. The owner of computer software has a variety of rights, including the ability to issue software licenses. Software licenses can be of various types.

2.5SOFTWARE LICENSES

2.5.1 Freeware licenses:

Freeware is proprietary computer software that is distributed for download and for an unspecified period of time. Freeware licenses are typically developed and distributed for free by software developers who wish to give back to the community. There are, however, certain restrictions. For instance, if you’re looking for a unique way to express yourself, try A freeware license that is nonexclusive, non-transferable, and has a restricted scope of use. Many freeware licenses stipulate that the applications cannot be used for commercial purposes. The license is non-exclusive, and it does not grant any operator exclusive privileges. Furthermore, the warrant is non-transferable, and the licensee is not permitted to assign any rights to a third party.

2.5.2 Open-Source Licenses:

As the name suggests, this license is available to anyone and has no limits. To be called “open source,” applications must satisfy a variety of criteria. Once an individual has created an open-source licence, the software must be freely distributed and redistributed. The owner of an open-source license cannot prohibit anyone from selling, altering, sharing, or using it for genetic analysis or other

purposes. The most basic interpretation is that open source licenses are legally binding arrangements between a software component's author and its owner, stating that the software can be used in commercial implementations under such circumstances. The license is what makes a piece of code open source. According to the terms and conditions, each open source license specifies what users are allowed to do with the program modules, their rights, and what they are not allowed to do. This may seem to be an easy job, but there are over 200 open source licenses to deal with, so good luck keeping track of them all. Organizations must select which licenses are more consistent with their practices to ensure that they remain legal, and these licenses vary in scope and specifications.

2.5.3 Shareware:

This type of app is also known as "try before you buy." For a limited time, this app normally comes with maximum availability. Users must either purchase the app or delete it from their machines at the end of the trial period. The trial date should be defined in terms of days. Shareware software is distributed at a minimal (or often no) rate, but complete legal use typically necessitates payment and registration. On a trial basis, copies are circulated. You have full freedom to test the app, evaluate if it suits your needs, and assess whether it is a decent deal. In most cases, order forms or ads contained in the program or on the delivery disk will instruct you how to register the program and how much it costs. A written manual, a modified copy of the software, often with added functionality, and the lawful right to use the program in their home or company are usually given to authorized users of shareware systems.

The developers of shareware applications receive reimbursement from those who wish to use the programs on a daily basis because it is not free software. It does, though, have the advantage over traditional consumer applications in that you can fully test a program before purchasing it.

Individuals or small businesses typically write shareware, and the content and level of service vary greatly. However, in some circumstances, shareware kits are generally more capable than equivalent commercial applications, and some commercial systems began as shareware.

Companies cannot charge premiums for copies that greatly outweigh their copying and storage expenses, even though shareware may be freely replicated. Shareware software writers hold rights to the contents, and you are not allowed to alter or distribute updated versions.

2.5.4 Demo ware:

Demo ware is only intended for use in demos. The prototype app has no usable functionality, and its primary purpose is to show the features to future customers. The owner of a software patent has the freedom to reuse and render as many copies of his work as he wants. Second, he might place his program on the internet, which would be called public view. He also has the rights to sell, rent, move, update, and change his proprietary software. Without the owner's consent, no one can use a copyrighted work for personal gain.

However, copyright infringement happens when someone uses a patented work for a commercial reason or to rob the author of income. Despite the fact that the software copyright owner has certain proprietary rights, they are not absolute and are subject to certain restrictions and exceptions in order to protect and preserve the public interest, including that of software users. Under certain socially desirable cases, the use of a copyrighted work is tolerated even without the author's consent.

In India, some acts that do not constitute copyright infringement include fair dealing with a literary, dramatic, musical, or artistic work for the purpose of private use, like study, criticism, or review, or making back-up copies purely as temporary protection against loss, destruction, or damage in order only to utilize the computer program for the purpose for which it was supplied.

2.6LET'S SUM UP

In this chapter, we have studied the types of online copyright violation along with a detailed study on its interface with cyberspace. Besides, we understood different provisions on copyright and types of licensing and their relevance in copyright.

2.7FURTHER READING

- Tabrez Ahmad, Cyber Law and E-Commerce, APH Publishing Corp., New Delhi, 2003
- Taubman, A. (2009), 'International Governance and the Internet', in: L. Edwards and Ch. Waelde (eds), Law and the Internet, 3rd ed, Oxford and Portland, Oregon: Hart Publishing, pp. 3-44

- Kolb, Arne (2009), ‘Protection of Computer Software’, in: L. Edwards and Ch. Waelde (eds), Law and the Internet, 3rd ed, Oxford and Portland, Oregon: Hart Publishing, pp. 335-360
- Kur, Annette, and Dreier Thomas (2013), European Intellectual Property Law, Cheltenham: Edward Elgar.
- Prytherch, R. (Ed.) (2005).Harrod’s Librarian’s Glossary & Reference Book. England: Ashgate. pp. 173, 543.
- Bailey, J. (2013). The Difference between Copyright Infringement and Plagiarism. Plagiarism Today. Retrieved November 29.

2.8 CHECK YOUR PROGRESS:POSSIBLE ANSWERS

1. What isOpen-Source Licenses?

As the word itself indicates, this license is open for all without any limitations. To qualify as “open source”, particular software must comply with several conditions. Once any person has developed such an open source license, then there must be free distribution, redistribution of such software.

2. What isPlagiarism?

Technological progress has made copying copyright material easy and simple. Consequently, the control of copyright infringement has very difficult and often impossible. Books, videos, films, music can be copied without any difficulty, and thousands of copies can be made from it and distributed.

3. What is the provision for data protection?

The Indian Copyright Act 1957 protects “Databases” as “Literary Works” under Section 13(1) a. Of the Act, which says, that copyright shall subsist throughout India in original literary, dramatic, musical, and artistic works.

2.9ACTIVITY

Provide detailed analysis of software licensing. (Word count- 2000-2500)

3

Unit 3: E-COMMERCE & ITS COPYRIGHT ISSUES

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Legal recognition to e-commerce practices

3.4 Issues of e-commerce

3.5 General issues

3.6 Protection to e-commerce

3.7 International frameworks

3.8 E-commerce protection in India

3.9 Let’s sum up

3.10 Further reading

3.11 Check your progress: Possible Answers

3.12 Activity

3.1 LEARNING OBJECTIVE

In this chapter we will learn-

- The E-Commerce regime and how it is treated under cyberspace.
- Concepts governing e-commerce including B2B, B2C, C2C etc.
- Various treaties and international conventions along with legal provisions.

3.2INTRODUCTION

E-Commerce is a revolutionary method of using digital information systems to conduct, manage, and execute company transactions. The Internet is available 24 hours a day, seven days a week, and from any place. The internet is the primary technology that allows all aspects of a commercial transaction (advertising, creation, acquisition, payment, and service delivery) to be done interactively with several people, without regard for time or space, in a multimedia (sound, picture, and text) environment at a low cost. Via the restructuring of conventional business, this allows changes in processes, resulting in considerable cost savings as well as improved productivity and efficiency. As a result, e-commerce is a commercial activity involving the use of hardware, operating applications, or computer networks. The Information Technology Act of 2000 was passed in order to give legal legitimacy to the idea of electronic banking, ecommerce, and electronic transactions, as well as to deter cybercrime and ensure safe practices. However, there are questions about intellectual PRoperty rights on the internet.[50]

Defining E-Commerce

The word "e-commerce" refers to "commerce dependent on bytes." Simply put, e-commerce is the electronic exchange of goods and services for a fee. E-commerce, in general, is a business methodology that meets the demands of enterprises, traders, and customers to cut prices while improving the quality of goods and services and speeding up service delivery. It's also known as the electronic data interchange, electronic fund transfer, and other terms for the paperless sharing of business records. E-commerce encompasses not only data exchanges but also

[50]Misra, ParthaSarathi, E-Commerce & Its Copyright Issues (April 3, 2011). Available at SSRN: https://ssrn.com/abstract=1801782 or http://dx.doi.org/10.2139/ssrn.1801782

general business activities such as public relations, advertising, agreements, contracts, and fund transfers. The Ministerial Declaration on E-commerce of the World Trade Organization2 (WTO) describes e-commerce as "the processing, distribution, selling, sales, or delivery of products and services through electronic means."[51]

Telephone, fax, television, electronic payment and money transfer services, EDI (electronic data interchange), and the internet are the six major E-Commerce instruments recognised by the WTO. E-Commerce, according to the European Commission, is more than mere internet browsing. It encompasses a wide range of activities such as shopping, searching the internet for products and services, collecting knowledge on things to buy, and completing purchases. It also includes the distribution and supply of certain goods and services, as well as investigations into order status. It also entails conducting consumer loyalty surveys, collecting information about customers, and managing consumer data bases for marketing campaigns and other similar operations, much as any other long-term commercial endeavor. E-Commerce creation is similar to a roller-coaster train. It's progressing, but it's not without its setbacks. It may be considered a part of the maturation process. The first phase of E-Commerce spawned a modern industry nomenclature focused on different permutations and variations of Business and Customers, such as Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Business (C2B), and Consumer-to-Consumer (C2C), and Consumer-to-Consumer (C2C) (C2C).

Business-to-Business (B2B)

It is a business platform that involves two separate or even dependent business actors, as the name implies. It serves as a business facilitator, negotiator, and dealmaker for mutually beneficial business units. For eg, Maruti, the vehicle manufacturer, has over 200 ancillary suppliers who finance its car manufacturing operations. It seeks their help (primarily in procurement) in keeping all of its pre- and post-production operations running smoothly.

Business-to-consumer (B2C)

It refers to a business network that links an organization with its customers. It is a retail version of E-Commerce that includes the sale of products or services through

[51] Ahmad, Tabrez&Misra, Partha. (2011). E-Commerce & Its Copyright Issues. SSRN Electronic Journal. 10.2139/ssrn.1801782.

online retailers. It is based on the idea of 'convenient shopping.' A customer can shop at his leisure, from any location and at any time. It's about a new kind of retail experience, one that involves an electronic version of catalog (mail order) shopping.[52]

Consumer-to-business (C2B)

It's a kind of retail marketing platform in which a company aggressively searches out or rather chases down consumers. It is a proactive version of e-commerce in the sense that it is a consumer chaser, selling consumers exclusive offers, packages, or packets of goods at cheap prices. Furthermore, it negotiates or bids on behalf of clients, including the best possible offers. Airlines and tour operators use it as a popular business model these days.

Consumer-to-consumer (C2C)

It reflects a consumer market network in which one consumer functions as a resource person, selling products to other consumers through an online channel for a fee. Market to consumer auctions are another name for this. This is an advancement on conventional sale or auction systems, which include a business-to-consumer partnership.

3.3LEGAL RECOGNITION TO E-COMMERCE PRACTICES

From the original introduction of UNCITRAL's Model Law on Electronic Trade by the United Nations General Assembly, e-commerce activities have come a long way in terms of legal approval. The UNCITRAL model law on electronic communications was created to promote the use of electronic commerce and to provide nations with model laws covering the use of alternatives to paper-based correspondence and data storage. It is built on a practical analogous approach which applies conventional paper-based standards such as printing, signature, and initial to a paperless environment. It recognizes electronic archives and digital signatures as legal documents.[53]

[52] Jane C. Ginsburg , Copyright Use and Excuse on the Internet, from papers.ssrn.com/sol3/papers.cfm?abstract_id=239747

[53] VikasAsawat, Information Technology (Amendment) Act, 2008: A new vision through a new change, from papers.ssrn.com/sol3/papers.cfm?abstract_id=1680152

On October 17, 2006, India became the world's twelfth country to adopt the UNCITRAL model legislation on electronic commerce. The model legislation on electronic commerce served as the basis for the Information Technology Act of 2000.

3.4ISSUES OF E-COMMERCE

Individual copies of a work kept in electronic media without the permission of the copyright holder constitute a copyright violation, according to a very simple formulation of how copyright laws in most countries apply to electronic communications. The main issue with this formulation in terms of ISPs and intermediaries is that the TCP/IP protocol that underpins the Internet, as well as the technology that overlay it, depend heavily, if not completely, on the ability to create copies of information.

3.5GENERAL ISSUES

Contractual Issues

(a) Online contracts are valid: The Indian Contract Act requires such contracts to be rendered in non-written formats. As a result, while internet contracts can be legitimate because they are assumed to be in these other ways, there are concerns about the legality of contracts that may be written down.

(b) Differences between normal and online contracts: It's important to understand the differences between normal and online contracts, especially when it comes to where and when the contract is signed. In this regard, the paper contrasts the UNCITRAL Model Law and the Information Technology Bill, 1998 to the dispatch and receiving of data messages under Indian law, based on the UNCITRAL Model Law and the Information Technology Bill, 1998.

(c) Evidence: According to the Indian Evidence Act, records must be supported by primary evidence, and the authenticity of data messages as primary evidence is debatable. There's also a question on how to access knowledge contained in machines.[54]

[54] Jaime Delgado & Isabel Gallego, Negotiation of copyright in e-commerce of multimedia publishing material, from elpub.scix.net/data/works/att/200129.content.pdf as accessed on 12th march, 2010.

3.6PROTECTION TO E-COMMERCE

As the Internet has increased in importance, copyright security has become increasingly relevant. For the past two decades, the copyright system has been continuously threatened by ever-increasing technologies, and the rule of copyright has emerged as a legal solution to those challenges. Copyright legislation has been modified to cover Internet products in the same way as it has been adapted to protect various other new mediums over the years. It safeguards original work as well as work that has been fixed in a physical form, such as printing, typing, or recording. Technologies like referencing, inlining, and framing, which are often used on the internet, pose a significant challenge to a right holder's copyright rights.[55]

3.7INTERNATIONAL FRAMEWORKS

The Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1995 were the foundations of international copyright law until recently. Since 1974, a separate United Nations body – the World Intellectual Property Organization – has been in charge of the universal copyright instruments (WIPO). WIPO's mission, as stated in its founding treaty, is to foster intellectual property rights around the world through international cooperation and, where applicable, partnership with other international organizations.

WIPO currently has 180 member states and administers six copyright treaties. Its aim is to harmonize national intellectual property rights in the long run, with the goal of creating a single, coherent body of international law.

The Berne Convention

As previously said, the Berne Convention was the first effort to harmonize copyright law on a global scale, and it was adopted in 1886. The Convention defined a minimum standard of copyright rights for member countries to adhere to, as well as a national care policy (under which a member state must give the same protection to material copyrighted in other member states as it gives to material copyrighted under

[55]Copinger and Sknoe James on Copyright, Volume 1 - By Kevin Garnett and Gillian Davis and GwilymHarbottle South Asian Edition 2008, 15th edition.

its own law). The treaty also provided that the International Court of Justice in The Hague (Hague Court) would have jurisdiction over disputes between member countries, but it also granted nations the possibility of claiming immunity from the jurisdiction, as many have done.[56]

Parallel to WIPO, the General Agreement on Tariffs and Commerce (GATT) has discussed copyright concerns. With the rise of the information society, copyright became profoundly important in influencing international commerce, leading the 1994 Uruguay Round of the GATT to create TRIPS – the Consensus on Trade-Related Facets of Intellectual Property Rights. The World Trade Organization was also founded during the same Round (WTO). In enunciating intellectual property rules, the TRIPS Agreement incorporates parts of the Bern, Rome, and Paris Conventions. Members shall conform with Articles 1 through 21 of the Bern Convention (1971) and the Appendix thereto, according to Article 9.1 of the TRIPS Agreement. Members, on the other hand, would have no privileges or responsibilities under this Agreement in relation to the rights conferred under Article 6bis of the Convention or the rights arising from it. As a result, it is clear that the path taken in the TRIPS Agreement's copyright clauses is to follow the Berne Convention's copyright protection regime. According to Article 10.1 of the Bern Convention, "Computer programs, whether in source or object code, shall be protected as literary works." Compilation of data or other material, whether in machine readable or other form, that constitute intellectual creations as a result of the collection or arrangement of their contents shall be protected as such, according to Article 10.2.[57]

World Intellectual Property Organization :(WIPO)

The World Intellectual Property Organisation (WIPO) is a United Nations agency (UN). Before its founding, a number of organizations such as the Assembly of Paris Union, the Executive Committee, and the International Bureau of Bern were created, all of which were later consolidated into the 'Bureau InternationauxReunis Pour La Defense de La ProprieteIntellectuelle,' or 'BIRPI.' Registration, fostering of intergovernmental collaboration in the management of intellectual property rights, advanced program operations, and, most recently, dispute resolution facilities are among WIPO's four types of activities. Member countries felt it was appropriate to

[56] Berne Convention, art 9(1): 'Authors of literary and artistic works…….shall have the exclusive right of authorizing reproduction of these works, in any manner or form'.

[57] Narayanan P., Copyright and Industrial Designs, Eastern Law House, 2010; pp 20 and 30

form a convention in 1996 to deal with the defense of copyright as emerging technologies evolved.

WIPO Copyright Treaty, 1996

On December 20, 1996, the Diplomatic Conference in Geneva accepted it. This treaty comes under Article 2 of the Bern Convention and is a special negotiation. It has everything to do with the Internet and new media. The WIPO copyright treaty is a special arrangement among WIPO member countries that gives authors greater rights than the Bern Convention. According to Article 4 of the Treaty, "According to Article 2 of the Bern Convention, computer programs are protected as literary works. Such safeguards apply to computer systems, regardless of their mode or type of speech." Furthermore, according to Article 5, "Compilations of data or other material, in some manner, that are covered as intellectual creations due to the collection or arrangement of their contents. This defense does not apply to the data or material itself, and it is in addition to any copyright that might exist in the data or material in the collection." The WIPO Copyright Treaty protects all types of programming systems, not just the object code or source code, as was the case in the TRIPS Deal. As a result, including the slight amendments introduced by the WIPO Copyright Treaty, it is not incompatible with the TRIPS Agreement.

The Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) was passed in October 1998 to carry out the US' treaty obligations under the WCT and WPPT, as well as to bring the country's copyright legislation into the digital age. The DMCA:

1. makes it illegal to circumvent anti-piracy measures built into copyrighted material, thus allowing the cracking of copyright protection devices for encryption research, product interoperability testing, and computer security system testing, and exempting non-profit libraries, archives, and educational institutions from anti-circumvention provisions under some circumstances.
2. Makes it unlawful to make, sell, or distribute code cracking machines that are used to unlawfully copy codes.
3. protects Internet service providers from copyright infringement liability for simply transmitting information, and limits the liability of non-profit institutions of higher education for copyright infringement by faculty members or graduate students while they serve as online service providers and in certain circumstances, thus requiring

service providers to exclude material from their systems that appears to constitute copyright infringement; and

4. Requires webcasters to pay record labels license fees.

3.8E-COMMERCE PROTECTION IN INDIA

In India, the Internet infrastructure is rapidly expanding. There are several questions about the internet. One of the most pressing problems surrounding the Internet, though, is the defense of intellectual property, or works of the imagination. Literary books, images, sound recordings, and other artistic works are protected from being reproduced without the consent of the copyright holder under Sections 13 and 63 of the Indian Copyright Act, 1957. It's also uncertain if copyright law would react to these materials when they surface on the site. The Copyright Act of 1957 makes no provision for ISP responsibility. Until now, India's stance on responsibility for copyright-infringing third-party content was unclear.[58]

With the advent of IT (Amendment) Act, 2008 there is a significant clarification regarding the scope of immunities available to intermediaries. Unlike the immunities under the old IT Act, these immunities are not only available with respect to offences under the IT Act, 2000 but even for the liabilities arising under any law. Section 79 of the IT Act exempts ISPs from responsibility for third-party information or data made accessible by them if the ISP has no idea of the violation or has used any reasonable efforts to deter it. Subject to the exceptions, an intermediary is not liable for any third-party records, details, or contact connection made available or hastened by him, according to the amended Section 79. Section 79 of the Information Technology Act of 2008 addresses ISP responsibility as follows:

The end of the(1) An intermediary is not liable for any third-party material, details, or contact connection made available or hasted by him, notwithstanding anything contained in any law currently in force, but subject to the provisions of sub-sections (2) and (3).

(2) The provisions of sub-section (1) shall apply if

(a) The intermediary's function is limited to providing access to a communication system in which third-party information is distributed, temporarily processed, or hastened; or

[58] The Digital Millennium Copyright Act - Overview , http://www.gseis.ucla.edu/iclp/dmca1.htm.

(b) The intermediary may not: (i) initiate the transmission, (ii) select the recipient of the transmission, or (iii) select or change the information contained in the transmission; and (c) the intermediary exercises due diligence in carrying out his responsibilities under this Act, as well as any other guidance that the Central Government may issue in this regard.

The exception to the above are:

1. The intermediary has conspired or aided in the wrongful act's commission; or
2. Upon actual discovery or warning by the proper Government or its entity that any content, data, or contact connection existing in or linked to a computer resource managed by the intermediary is being used to perform the unlawful act, the intermediary fails to delete or disable access to the material on that resource without tarnishing the proof. In the two scenarios mentioned above, the ISPs will be held accountable. The additions to Section 79 of the IT Act provide a non-obstinate provision, which states that "notwithstanding everything inherent in any statute for the time being in effect," and thereby protects ISPs from liability resulting from such laws.

At the same time, the amended section 81 contains the following proviso: "Provided that nothing in this Act shall prevent any individual from exercising any privilege granted under the Copyright Act, 1957, or the Patents Act, 1970." The aim of this provision, according to the understanding, is to maintain the priority of the Patent Act and the Copyright Act over the Information Technology Act. We can correlate the section 79 and 81 by inferring that other legislation is Copyright Act. Both the section counter each other but a careful and finer study will justify that the section 79 has been amended to give more relaxation to ISPs.

Section 79 of the amended act has been framed in accordance with EU Directives on E- Commerce to determine the extent of responsibility of intermediaries for third party data or content. The objective of the directive is to promote free flow of information between the member states. The EU Directive spells out the intermediaries' responsibilities in great depth, including not only intellectual property rights and related obligations, but also general material responsibility. The EU Directive on Electronic Commerce was created with the aim of developing information society services (ISS), ensuring regulatory certainty and customer trust through the coordination of national legislation, and clarifying legal principles for the

proper functioning of the internal market in order to provide a legal structure that allows ISS to freely travel between Member States.

Under the E-Commerce Directive, an ISP is exempt from liability when it serves as a "mere conduit" (Article 12) or provides "temporary caching" (Article 13) for the sole purpose of making the transmission of content more efficient, is of a mere technical, automatic and passive nature, and where the ISP has neither knowledge nor control over the content being transmitted or stored. The terms under which a hosting company is immune from responsibility, as specified in Article 14(1)(b), serve as the foundation for the development of "alert and take down" procedures by copyright owners to ISPs in order to resolve instances of infringement.

3.9LET'S SUM UP

In this chapter, we have learned the laws on copyright under E-commerce and the international regime governing the same. Besides, along with legal provisions we have understood the terms like B2B, B2C, and C2C etc.

3.10FURTHER READING

- Nimmer on Copyright, Lexis Nexis, Melville B. Winner & David Winner, Indian Print 2010. Copinger and Sknoe James on Copyright, Volume 1 - By Kevin Garnett and Gillian Davis and GwilymHarbottle South Asian Edition 2008, 15th edition.
- Legal Dimensions of Cyberspace, S.K. Verma& Raman Mittal, Indian Law Institute, 2004.
- Dr. Wadehra B.L., Law Relating to Intellectual Property, Universal Law Publishing Co., 4th Edition

3.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Business-to-consumer (B2C)?

It refers to a business network that connects a company with its customers. It is a retail version of E-Commerce that includes the sale of products or services through online retailers. It is based on the idea of 'convenient shopping.' A customer can

shop at his leisure, from any location and at any time. It's about a new kind of retail experience, one that involves an electronic version of catalog (mail order) shopping.

***2*. What is Consumer-to-business (C2B)?**

It's a kind of retail marketing platform in which a company aggressively searches out or rather chases down consumers. It is a proactive version of e-commerce in the sense that it is a consumer chaser, selling consumers exclusive offers, packages, or packets of goods at cheap prices. Furthermore, it negotiates or bids on behalf of clients, delivering the best possible offers. Airlines and tour operators use it as a popular business model these days.

3.12 ACTIVITY

Elaborate on international conventions and treaties governing E-Commerce. (Word count- 2000 to 2500).

Unit 4: COPYRIGHT PROTECTION IN CYBERSPACE- A COMPARATIVE STUDY OF USA AND INDIA

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Laws- a comparison

4.4 USA

4.5 India

4.6 Compliance with International regimes

4.7 Liability on infringement

4.8 Let's sum up

4.9 Further reading

4.10 Check your progress: Possible Answers

4.11 Activity

4.1 LEARNING OBJECTIVE

In this chapter we will learn-

- The comparative analysis of USA and India in light of its copyright provisions.
- The compliance regime in USA and India with respect to copyright infringement.
- Various legal provisions governing copyright in national and international forums.

4.2INTRODUCTION

It has aided globalization significantly by promoting the quick sharing of information from one location to another, resulting in increased communications and awareness dissemination.[59] Every year, about 8,50,000 objects, including books, magazines, electronic, and multimedia materials, are published worldwide, according to UNESCO. However, it has also been seen to be dangerous in certain instances. Copyright laws are designed to strike a balance between the author's private rights and the public's overall interests. However, with the emergence of the internet and cyberspace, it is impossible to draw a straight distinction between the public's needs and the author's interests. It has greatly helped in globalization by facilitating easy exchange of information from one place to another thus leading to increase in communications and spread of knowledge. According to UNESCO, approximately 8,50,000 items which include books, journals, electronic and multimedia resources are published worldwide every year.[60] But, it has also proved to be harmful in some ways. Copyright laws are aimed at maintaining a balance between the individual interests of the author and the interests of the public at large.[61]However, with the coming of the internet and the advent of cyberspace, it is difficult to draw a clear line between the interests of the public and the interests of the author. It has led to the commission of certain crimes in a much hassle free manner than executing them in

[59]R MurugaPerumal, Copyright Infringements in Cyberspace: The Need to Nurture International Legal Principles, 14(3) INTERNATIONAL JOURNAL OFTHE COMPUTER, THE INTERNET AND MANAGEMENT 8,8 (2006)

[60] Frank Pasquale, Toward On Ecology of Intellectual Property: Lessons from Environmental Economics for Valuing Copyright Commons, 8 YALE J.L. & TECH 78, 110 (2006)

[61]Muragendra B.T., Copyright and Trademark in Cyberspace, 3 (6) International Journal of Scientific and Engineering Research 1, 2 (2012)

person. Infringement of copyright is one of such wrongful acts. Earlier, the infringer had to do all acts physically so it was easy to locate him, but through a large number of networks in cyberspace, it is not even possible to track the offender or stop such infringement every time it occurs. Therefore, digitalization has a profound effect on creation, reproduction and dissemination of works protected by copyright. Now almost anything or everything can be transmitted on cyberspace. Movies like Star Wars and Spiderman could be downloaded easily before they hit the screens, mainly due to the advent of digital technology. In the light of these situations, almost every country has felt the need for developing and enacting effective laws to prevent loss to the authors due to mass undetectable copyright infringement. The laws have been discussed below in detail.

In the world of digitalization, the problem of copyright infringement in cyberspace has become a big challenge. There are several reasons for this; one such reason is in my opinion, the level of enforcement of copyright laws in the countries. So, to confirm this viewpoint, a detailed study will be made of the legislations that have been enacted in the two countries selected for study- USA and India, one with a strongly developed copyright law and one with a comparatively developing copyright law.

4.3LAWS- A COMPARISON

The comparison of the laws of the two countries USA and India has been made on various aspects of the law as discussed below:

Jurisdictional Issues The question of jurisdiction of courts in case of copyright infringement in cyberspace is a matter of global debate due to the unique nature of dissemination of information through the internet.

4.4 USA

It is relevant to mention that USA is the first country where computer software were developed, so naturally the country had to bear the burden of incidents of intellectual property infringement in cyberspace before any other country. As these incidents were on an increase, the US courts had to exercise their powers to give justice to the victims of copyright infringement. Since 1990s the Courts have developed two tests for determining their jurisdiction to entertain complaints of intellectual property

infringement. The first test referred to as the Zippo test was developed in the case of Zippo Manufacturing Co v Zippo Dot Com Inc[62].

The test based jurisdiction of the US courts on the extent of a website"s „interactivity" in the given jurisdiction. In the opinion of the Court, "a passive website is insufficient to establish personal jurisdiction, but an interactive site through which a defendant conducts business with forum residents, is sufficient to establish personal jurisdiction." But a major drawback of this test was that it did not provide any guideline as to what amounted to the right level of interactivity in order to constitute jurisdiction, whether a continuous day to day record is required or it is sufficient to show a fairly regular interaction. The second test also referred to as the "effects test" was given in the case of Calder v Jones.[63]

The test based jurisdiction on three criteria: (1) an intentional action (2) expressly aimed at the forum state (3) knowledge that the brunt of the injury would be felt in the forum state. Thus, it indicated that if the person being affected by the copyright infringement or the spread of the copyrighted work is widespread in the forum state, it has full jurisdiction over the matter. Although the second test is not much in use today, the first test does have a great significance in determining jurisdiction in recent infringements. A recent case of United States v Kim Dot Com[64] that decided the jurisdiction in case of a matter under the DMCA 1998, gave quite a similar view. The Court was of the opinion that „corporations that are foreign in their registration and address but conduct a substantial amount of business in the United States will not be able to dodge the jurisdiction based on formalities". The courts have however become a bit more flexible in this approach and do not always look for a high amount of business. This is reflected in the case of Inc v Yandex NV[65] where a Dutch search engine was held to be subjected to the California Court even though only 6 per cent of the infringements occurred in the United States.

4.5 INDIA

The Indian law is not very clear in this regard. Section 62(2) of the Indian Copyright Act, 1957 confers an additional jurisdiction to the courts to take cognizance of

[62] Justice S Muralidhar, Jurisdictional Issues in Cyberspace, 6 THE INDIAN JOURNAL OF LAW AND TECHNOLOGY 1,1 (2010)
[63] 952 F. Supp. 1119 (W.D. Pa. 1997) (US District Court)
[64] 465 U.S. 783 (1984) (US Supreme Court)
[65] 2012 WL 517537 (E.D. Va. Feb. 16, 2012) (US District Court for the Eastern District of Virginia)

matters of infringement of copyright over the internet by providing for an extra place of suing other than the grounds provided under Section 20 of the CPC, 1908.[66]Thus, such infringements can be brought within the purview of District Courts under Section 62. This again raises a very crucial question as to the constitutionality of Section 62(2) of the Act as it would mean extraterritorial jurisdiction of the courts which is clearly in conflict with Article 1(2)[67] of the Constitution of India, 1950.

Although the IT Act provides for all cyber laws, it does not particularly the problems of intellectual property rights. So, provisions do not indicate any solution. However, the Indian judiciary has read in jurisdiction of the Indian courts in these provisions. In the case of Super Cassettes Industries Ltd v Myspace Inc&Anr.,[68] the use of the words „any place" for profit under Section 51(a) of the Copyright Act, 1957 have been interpreted to include common public place or library or any other kind of place. It subsumes within it physical place or place at the internet or web space.

A landmark case is that of Banyan Tree Holdings Ltd v M Murali Krishna Reddy and Anr.[69]in which the issue of extended jurisdiction was dealt with. The plaintiff here was a resident of Singapore and the defendant was from Hyderabad. The rationale of Casio India Ltd v Ashita Tele Systems Pvt. Ltd.[70] was relied upon to conclude that due to the ubiquity, universality and utility of the features of the Internet and the Worldwide Web, any matter associated with it possesses global jurisdiction. The Court also relied on the holding in Zippo Manufacturing Co v Zippo Dot Com[71]and some other US decisions and concluded that the Court did have the jurisdiction to deal with the matter.

4.6 COMPLIANCE WITH INTERNATIONAL REGIMES

For addressing the problems of intellectual property infringement over the internet, various international regimes were developed. The World Intellectual Property Organization Internet Treaty was one of its kinds. Both USA and India are signatories to WIPO. It is pertinent to check their incorporation of the treaty into their domestic laws.

[66] 2013 WL 1899851 (N.D. Cal. May 7, 2013) (US District Court)
[67] Section 62, Copyright Act, 1957
[68] (2011) 48 PTC 49 (Delhi High Court)
[69] 280 F.3d 934 (9th Cir. 2002)(US District Court for the District of California)
[70]Abhai Pandey, Inside Views, Development in Indian IP Law: The Copyright (Amendment) Act, 2012, Intellectual Property Watch (January 1, 2013), available at http://www.ip-watch.org/2013/01/22/development-inindian-ip-law-the-copyright-amendment-act-2012/
[71] Berman, CAREER GUIDE TO INDUSTRIES, 2008-09 143 (2008)

USA

In USA the Digital Millennium Copyright Act was enacted in 1998 to bring the Copyright Act in consonance with the provisions of WIPO treaties. Section 1201 of the US Copyright Act, 1976 added by Section 103 of DMCA protection against circumvention of technical measures used by copyright owners to protect their works. Two types of technological measures have been recognized: measures that prevent unauthorized access to a copyrighted work and measures that prevent unauthorized copying of the copyrighted work. The circumvention of the first was prevented but not the second, in order to promote fair use These changes were made in consonance with Article 11 of WCT and Article 18 of WPPT. In this regard, the US Court has held in the case of Kelly v Arriba Soft Corp[72] that providing thumbnail versions of images and automatic indexing of webpages containing images will amount to fair use. Similarly, Section 1202 was added to protect the integrity of copyright management information in consonance with Article 19 of WPPT.

INDIA

In 2012 the Copyright Act of 1957 was amended to bring it in consonance with the World Intellectual Property Organization Internet Treaties- the WCT and WPPT. Along with providing for technical measures to protect copyrighted works in cyberspace, it also provides for special fair use provisions for works in the internet. The word “hire” was included in Section 14 of the Indian Copyright Act, 1957 in compliance with Article 7 of WCT and Article 9 of the WPPT, which provide for “commercial rental” rights for computer programmes and cinematograph films. In Section 14(d) and (e) the term “hire” was replaced by the term „commercial rental‟ in order to narrow down the scope of hire to only commercial rentals and not non-commercial ones. The definition of the term commercial rental was also introduced under Section 2(fa) of the amended Act. Fair use provisions are now extended to digital works.

4.7LIABILITY ON INFRINGEMENT

In case of copyright infringement over the internet, multiple parties are involved in the act. The parties involved in copyright infringement over the internet are: copyright

[72] 464 U.S. 417, 435 (1984)(United States Court of Appeals)

owners, internet service providers and the individual involved in uploading the copyrighted material in the server of the Service Provider. ISPs (internet service providers) are organizations that provide their clients or customers with access to the internet. It generally appears that the person uploading the document should be responsible for infringement, but there is a tendency to rather hold the service provider liable for infringement. There are mainly two reasons for this: 1) due to the wider reach of cyberspace it is difficult to locate an individual who actually uploads the copyrighted material, whereas the service provider is an organization having its place of business in a definite place, 2) an individual will not be able to pay the amount on infringement but an organization can pay for making good the losses on infringement. This trend is also visible in the laws of two countries for fixing liability:

USA

In US the liability for copyright infringement in cyberspace has been established with the help of case laws. One of the initial cases is that of Sony Corp v Universal Studios where the Internet Service Providers were held liable by virtue of vicarious liability and contributory infringement. Later, in the case of Religious Technology Center v. Netcom Online Communication Services, Inc. the Federal District Court of Northern California was posed with a similar question of liability of the ISP for a material posted by the clients. The court adjudged on three main issues: firstly, Netcom could not be directly held liable for the material posted directly by its clients. In its opinion, the ISP is the one, which only provided the tool, and the original infringing work was done by the client who uploaded it.

This was a clear dissent from the previous judgements in this regard. Secondly, the link between the infringing activity and Netcom's finances were not sufficient to hold Netcom vicariously liable. Thirdly, though Netcom could not be held liable for direct infringement or even vicariously, it could be definitely made liable for contributory infringement. This however had to be proved, which was left open for trial, and the case was subsequently settled out of the court.

INDIA

The stand in India is completely opposite to that of USA. There is no definite law or decision which provides guidelines for such kinds of infringement. A small provision can be said to have been made in the Information Technology Act, 2000 by virtue of Section 79 of the Act, which exempts the internet service provider from liability in case of third party violations, if due diligence is proved. However, confusion arises as

to the specific position of copyright infringers within the text of this provision. The words „under this Act, rules or regulations made thereunder indicate only a bar under this Act and not that of the Copyright Act. In such a situation, it is important to look at various case laws in this regard in India. The judicial response suggests that the ISPs have been held liable for acts of contributory infringement, not following the provisions of the IT Act, 2000. In one case of Super Cassettes Ltd v Yahoo Inc and Anr, the Delhi High Court had issued a notice to the ISP Yahoo Web Services (India) Pvt. Ltd for infringing copyright of the plaintiff by streaming one of its videos in the portal video.yahoo.com. The Delhi High Court has issued similar notice to other ISPs like Google, Youtube. Some amendments have also been brought about in the Act in Section 52(1) (c) for restricting liabilities. However, there is still no express provision.

4.8LET'S SUM UP

In this chapter, we have learned the laws of two countries-USA and India in the light of copyright protection of their works in cyberspace. The main issues revolved around the jurisdiction of domestic courts, compliance with WIPRO, liability on infringement and remedies for the copyright owner. We have also learned various laws and the decisions of the courts.

4.9FURTHER READING

- Thomas H Davenport, INFORMATION ECOLOGY: MASTERING THE INFORMATION AND KNOWLEDGE ENVIRONMENT, 3 (1997)
- Tatiani G Rapatzikou, GOTHIC MOTIFS IN THE FICTION OF WILLIAM GIBSON, 100 (Rodopi,2004)
- [3] ChitrarekhaKuffalikar, Redefining IPR in the New Digital Environment: Some Concepts For College Libraries in INTELLECTUAL PROPERTY RIGHTS AND COPYRIGHT, 50, 51 (SP Satarkar ed., 2003)
- JJ Hua, TOWARD A MORE BALANCED APPROACH: RETHINKING AND READJUSTING COPYRIGHT SYSTEMS IN THE DIGITAL NETWORK ERA, 39 (2014)

- Super Cassettes Ltd. v MrPunitGoenka and Anr. 2009 (41) PTC 1(Delhi High Court)
- Frank Pasquale, Toward On Ecology of Intellectual Property: Lessons from Environmental Economics for Valuing Copyright Commons, 8 YALE J.L. & TECH 78, 110 (2006)

4.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the reasons to hold the service provider liable for infringement?

There are mainly two reasons for holding service provider liable.

1) due to the wider reach of cyberspace it is difficult to locate an individual who actually uploads the copyrighted material, whereas the service provider is an organization having its place of business in a definite place,

2) an individual will not be able to pay the amount on infringement but an organization can pay for making good the losses on infringement.

2. State the criteria to determine the jurisdiction.

There are three criteria: (1) an intentional action (2) expressly aimed at the forum state (3) knowledge that the brunt of the injury would be felt in the forum state. Thus, it indicated that if the person being affected by the copyright infringement or the spread of the copyrighted work is widespread in the forum state, it has full jurisdiction over the matter.

4.11 ACTIVITY

Elaborate on the jurisdiction of domestic courts, compliance with WIPRO, liability on infringement and remedies for the copyright owner (Word count- 2000 to 2500)

Block-3

TRADEMARK AND CYBER LAW

1

Unit 1: TRADEMARK TRAFFICKING IN CYBERSPACE

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Cyber spacing

1.4 Fundamental of Trademark

1.5 Rights under Trademark

1.6 Trademark in cyberspace

1.7 Linking and framing

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVE

In this chapter we will learn-

- The traditional notion of trademark law and its shift towards cyberspace.
- Relevant case laws in relation to determination of the jurisdiction of the case.
- Various remedies in case of trademark violation on cyberspace.

1.2INTRODUCTION

Unimaginable growth of the Cyberspace raise the various thought in trademark related issues arises in it. Many of the issues are solved by the traditional notion of trademark law, whereas the other present thornier questions requiring greater sensitivity for the effecting marketing in internet. The domain name dispute is the cyberspace trademark issue that continues to attract the most coverage. Is a domain the same as a trademark? When does a domain's use infringe on a trademark's rights? What will a corporation do if someone else registers its name or trademark as a domain name? Beyond domains, there are a slew of trademark problems that are sure to outweigh domain conflicts in the end. Along with the internet, questions about what constitutes patent use and misuse are exploding. Companies must be cautious in minimizing trademark dilution and think carefully before linking to other sites or allowing others to link to the company's site using company trademarks, in addition to standard trademark improvement and policing issues that take on new forms on the Internet. Attempting to enforce trademark rights in cyberspace is a difficult but fascinating job.[73]

1.3CYBERSPACING

Cyberspace is a futuristic computing environment and an interactive medium that is used to link computers all over the world. Cyberspace is a global computer network that uses the TCP/IP protocol to allow online networking and data transfer. The term cyberspace was initially introduced by William Gibson in his 1984 books, “Neuromancer”. Later on it was Gibson who criticizes the term in late year, calling it

[73]Meena Amar, lectures on Cyber Laws, 1st ed. (Hyderabad: Asia Law House, 2011), pp.71 to 72.

evocative and essentially meaningless. Cyberspace allows users to share information, conduct business and many other activities. It mostly gained its interest not by its technical execution and implementation but by the social interaction. The Cyberspace does not have any physical foundation that we used in the real world. But that virtual effect in cyberspace takes place in the real world have a real effect. Cyberspace, according to author Bruce Sterling, is "the location where a telephone call seems to take place."[74] It's not in your phone; it's in the plastic unit on your desk. Not in the other person's house, but in a different city – the space between the phones. The indefinite location where the two of you, as human beings, meet and communicate." The growth in the internet brought the problem in the cyberspace because of its ease flow of information and communication led the misuse of the information in the internet. In fact, the investigator has revealed that the incident of 9/11in the U.S.A and the 26/11 in Mumbai are result of the internet where the carnage communicates to each other through the internet.

1.4FUNDAMENTALS OF TRADEMARK LAW

Trademark law Trademark is the word, symbols, or phrase of the particular manufacturer or seller's product distinguish itself from other product. For example the TM of Nike is different from other brand of the shoes such that in internet is done by Nike.com and under some circumstances the packaging and procedure also include in the trademark. Trademark is very much essential in industry and commercial business to of identify their product. This trademark secures the right of the owner of the manufacturer and avoids the infringement of the product so that no person can allow using that mark with approval of the owner. The trademark is the way by which right of both the consumer and manufacturer owner. The essential function of the trademark is to identify the origin of the consumer source and the product source. It is properly called as indicate source or serves for example, "Pepsi", "coke cola", "McDonalds" etc. Trademark is an essay way to the consumer to identify the product source.[75] Trademark just directly looks in the symbols of the

[74] R.K. Chaubey, Cyber Crime and Cyber Law, 1st ed. (kolkatta: Kamal Law House, 2008), pp712 to 714

[75] See Joe Mullich, Coffee Break: Some Play Net Domain Game Hoping for Big Gain, BUSINESS FIRST, Aug. 25, 1997, at 18. The results of a 'whois' search on conducted on January 28, 1999, indicate that the domain is still registered to Khoshnood but evidently does not have a server location.

product from which a consumer can easily know the quality of the product. For example if the person has to buy cold drink, he simply sees the symbols of Pepsi and borrows it. Such that in internet the consumer directly look into the domain name example when a person have to buy cell phone he will look into the application of flip kart which assured the safe delivery of the product.

1.5RIGHT IN TRADEMARK

Right of TM owner – the trademark owner has three essential rights: 1. Exclusively right to use that product. 2. To obtain relief from the infringement of the product. 3. Right to assign the TM in consideration to use. The right in the trademark are confer by two ways that is by registering the trademark in registration office i.e. patent and registration office or by being the first one to use that trademark in commerce.[76] The use of marks means the actual sale of the product to public in that area where it gain the reputation for example if owner sale pizza in his local area than he gain the reputation over there and can protect that marks from the late comers who use that marks. But if the mark is used in other geographical area then the mark could not called as infringes. The other way to use mark is by registering that mark in the registration office. It is the bonafide intention to use that mark. After the marks have been registered the right will be confers to sue the party in infringement or could claim the remedy from that person. This right is limited if the mark is been used in geographical area then the registration owner of the trademark can use that mark everywhere except in that area where it has been used earlier.

1.6TRADEMARK IN CYBERSPACE

Traditionally, trademark law was used to shield merchants who had registered trademarks by granting them exclusive rights to do business under the logo and excluding third parties from doing so. However, with the advent of the internet and the paradigm change from the conventional trading method to the online forum, the

[76] McCarthy J Thomas, Dilution of a trademark: European and United States law compared in Intellectual Property in the New Millennium, 165-166

traditional trading process has become obsolete. Many new problems have arisen in the area of trademark rights.

One of the most prominent places where trademark disputes in cyberspace occur is the domain name. A domain name is essentially the name given to a website; it is similar to an address that people use to access the website. The domain name is very significant in device recognition, and is achieved with the help of an IP address, which is a series of numbers and letters. However, due to the IP address's complicated numeric coding, simpler alternatives that are easily remembered have been created. A domain name is an option that may be a mixture of words, symbols, and numbers. For instance, a domain name may be www.lawyerswork.com.[77]

It is vital to register a domain name in order to create a structured marketable position on the internet. As a result, there is no trademark examination of domain names because it will be too much hassle for the registrar. As a result, there are four situations in which a controversy over a domain name versus a trademark occurs.

The first instance is known as cyber-squatting. It applies to the act of registering a domain name for the purpose of conducting trade and commerce. The domain name is the company's trading name, but it is not registered with the company. A third party registers a domain name with the intention of transferring it to the original owner for a fee. The applicant cannot file his trademark as a domain name until the other party has the domain name, and therefore his right to register is infringed. It has been noted that a domain name serves as a company's identifier. It has the same purpose as a company's trademark. A domain name is more than just a way to get to a certain website.

Furthermore, if an entity registers a domain name that is equivalent or close to a trademark of a corporation for which he has no business relationship, an injunction can be issued against the person. There was no legislation pertaining to domain name rights. The United States was the first nation to pass laws on the subject. The Cybersquatting Piracy Act of 1999 was the name of the law.

---

[77] Further complications arise with regard to user names and subdomains. Although NSI may assign second level domains, domain holders are free to create any number of subdomains and user names. Thus, the journalist who registered , in part to call attention to the reality that only the affluent have access to the Internet, used the moniker 'Ronald' (ronald@mcdonalds.com). See Joshua Quittner, Billions Registered, Wired Magazine, October 1994 (visited April 22, 1999) . Likewise, there was nothing, other than trademark law, to prevent the registrant of the domain from using a subdomain such as 'microsoft' () even accompanied by the user name 'gates' (gates@microsoft.windows95.com).

The cyber parasite is the second case, in which benefits and profits are gained through the use of the real domain name. The approach entails using a generic or misspelled domain name that is similar to a well-known trademark. These strategies are used to trick customers to pawn off goods as their own. In the case of Rediff Communication Ltd. v. Cybertooth and Others, the defendant had registered a domain name that was confusingly similar to the plaintiff's and was operating a similar company. The defendant intended to carry out his trade and business under the plaintiff's trademark or trade name, resulting in a violation of the plaintiff's privilege, according to the court.

The Cyber twin is the third scenario. This condition happens where all parties to a lawsuit have a legal right to a certain domain name.

Reverse cyber-squatting is the fourth case involving a domain name. This is the antidote to cyber-squatting. It entails trademark owners attempting to take control of a domain name by using tactics such as bogus cybersquatting claims against the domain name's legitimate owner. To avert legal repercussions, the domain name owner is required to pass the domain name to the trademark owner.

Apart from the above obstacles, there are also several other cyberspace challenges posed to a company's trademark. In the cyber space, another field where a trademark dispute can occur is hypertext connections. It basically refers to moving a user from one page of a website to another. There are hyperlinks that are inserted between web pages. For eg, we can see a hyperlink for ‘Gucci' on a web page, but when we click the link, we are taken to another web page that may sell similar items but is not associated with the brand Gucci. Trademarks are infringed as a result of these hyperlinks. Furthermore, it is simple to monitor the hyperlinks that exist in cyberspace. As a result, a functional solution in this area has yet to be formulated.

In certain cases, the use of keywords may result in trademark infringement in cyberspace. Often times, web sites use well-known trademarks as keywords in order for their website to appear at the top of the search results. The use of a trademark can mislead an unsuspecting user, resulting in infringement.

The internet was initially created as a tool for communication only for government and industrial purpose but now it becomes the global economic purpose. The easy flow of information and ease of communication increase the ability to access the information which creates the opportunity to misuse and criminal activity. It had tremendous impact in intellectual property. Domain name dispute is the most active

part that involves the accusation of trademark infringement usually by the cyber squatter. Recently there was no law regarding the protection of the domain name but after the legislation made by the United State, which is the first country to make cybersquatting infringement act 1999. In an increasingly global market the brand become important for competitive advantage in the internet. ”Brands rely on their symbolic power to draw attention to themselves and build an acknowledged capacity for value creation”. Brand can secure its rights by registering the trademark as a domain name. The current internet technology does not limit problem of cybersquatting and other confusion regarding the TM as a domain name.

With the adoption of the Domain Name Dispute Resolution Policy (UDRP) on August 26, 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) created a new regulation. The Internet Organization for Assigned Names and Numbers (ICANN) is in charge of maintaining and organizing the domain name scheme to ensure that each address is unique, including IP addresses and domain names. Via its Digital Agenda, which combines the internet, digital media, and the intellectual property regime, the World Intellectual Property Organisation (WIPO) guarantees that the rights of authors and owners of intellectual property are secured around the world.

Cyberspace is functioning well in order to effective commercial marketing and business but with this the right of consumer and owner of product must be protected. The development of law in the technical field is limited but with little courage the law and technology together will protect the trademark community in cyberspace. The most common aspect of domain name issue issues is that of cyber squatting. Under the U.S Anti-Cyber squatting Consumer Protection Act 1999, cyber squatting is the use of trademark in order to take advantage by that trademark and by registering domain name of the famous company to take undue benefit from it. One of the corollary of the cyber squatting is typo squatting where the users are made to make a typographical errors when entering in the domain name. For example:

1. BSNL.co.in into BSNL.com
2. Sony.com into soni.com
3. Facebook.com into facebok.com

*Yahoo Inc. vs. Akash Arora 19 feburary1999*The appellant, who is the registered owner of the domain name "yahoo.com," was successful in securing a temporary injunction prohibiting the defendants and their associates from doing business on the

Internet or elsewhere under the domain name "yahooindia.com" or any other trademark/domain name that is confusingly identical to the plaintiff's trademark.
Domain Active Property Ltd Sbicards.com vs. Sbicards.com was requested by the World Intellectual Property Organization (WIPO) to be sold to an Indian company from an Australian firm that had stolen the domain name in the hopes of selling it for a large amount to a State Bank of India affiliate later. SBI Card's claim that the Australian firm was in the business of buying and selling domain names from its website was acknowledged by the panel.[78]

1.7LINKING AND FRAMING

Hyperlink is the transportation of the users to another location. Linking create problem with feature like “deep linking” and in the framing helps the site manager to create frames on the page itself and open web page on a single page. It makes vulnerable to intellectual property right violations. Meta tagging is another major problem for the trademark holders. Meta tagging containing the words, keywords and content of the pages due to its meshing of the technology makes its legal issue. It signify the HTML, which forms the basis of the WWW.[79]

- Remedies International level
- Provision of the Anti cyber squatting consumer protection act (1999).
- International arbitration system created by ICANN.
- National level
- National internet exchange of India
- WIPOs and arbitration system
- Suit in ICANN

Jurisdiction and enforcement

Anti cyber squatting Consumer Protection Act (ACPA) feature is that it enables in rem jurisdiction in domain name dispute which means that the domain name owner does not have to sue personally but can takena action against domain name itself. But it is not easy to sue the cyber squatter as the location of the infringer could not

[78] Mariela Maidana-Eletti, Market Access and Trademark Protection in the WTO Regime: The Case of Certification Marks, RECHT UND GESUNDHEIT: JUNGE RECHTSWISSENSCHAFT LUZERN 69, 82 (2013), available at http://ssrn.com/abstract=2602000.
[79] NEIL WILKOF & DANIEL BURKITT, TRADE MARK LICENSING, 176–78 (Sweet & Maxwell 2d ed. 2005).

be located then the person cannot be sue as in context of the U.S. law. To take advantages of the rem provision the trademark owner must have to satisfy that the location of the infringer could not be found. The plaintiff in rem provision cannot claim damages but the remedies to cancellation or transfer of the domain name in related matter the TM owner prefer the (ICANNs) Uniform Dispute Resolution policy. Thus the above policy cannot provide the damages claim. For such that the plaintiff has to sue the cyber squatter personally for damages. But such policy is silence in the dispute which is outside of their jurisdiction and the internet community has to take more skill technique and effective implementation of law in the cyberspace in order to protect the TM in internet.

Therefore, it can be concluded that the protection of trademark in the cyberspace is very complex subject and it is very difficult to stop the infringement of trademark as the internet is so much vast in nature, involving many grey area which have to be focused in order to protect the right of TM owner. Our existing law doesn't have the effective remedies to plaintiff as the infringer location could not be found and the out of jurisdiction could not be sued. Such failure could amount to destruction in the global market. Legal right of an individual poses the challenge for the court to secure the physical presence of the party who is located outside the jurisdiction of the respective court and enforce it. All the concerned authorities working towards betterment of healthcare facilities should work together and take steps to provide:

- Remedies to the plaintiff
- Implementation of law where it is not possible
- 26Protection of trademark community in cyberspace

1.8 LET'S SUM UP

In this chapter, we have learned the laws on trademark and its related aspects of trafficking. We have also covered relevant case laws along with its reference in Indian context. We have also understood the remedies and steps to mitigate the trademark trafficking,

1.9FURTHER READING

- Jonathan Eisenberg, A Guide to the Anti cyber squatting Consumer Protection Act, 2000. www.gcwf.com/articles /journal/jil-march00-1.html

- Jonathan Eisenberg, A Guide to the Anti cyber squatting Consumer Protection Act 2000. www.gcwf.com/articles/ journal/jil-march00-1.html
- Christopher R Perry. Trademarks as Commodities: The 'Famous' Roadblock to Applying Trademark Dilution Law in Cyber space Connecticut Law Review, 2000; 32:1127
- Jack Goldsmith. Cybercrime and Jurisdictions, 2000.
- David Post. Governing Cyberspace This article was to appear in Fall 1997 in Wayne Law Review. F. Gregory Lastowka, Search Engines, HTML, and Trademarks: What's the Meta For? 86 Virginia Law Review, 2000, 835.
- David Streitfeld. Making Bad Names for Themselves; Firms Preempt Critics With Nasty Domains The Washington Post, Friday September 8, 2000, Westlaw 25414864

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is cyber spacing?

Cyberspace is a futuristic computing environment and an interactive medium that is used to link computers all over the world. Cyberspace is a global computer network that uses the TCP/IP protocol to allow online networking and data transfer.

2. What are the rights of trademark owner?

The trademark owner has three essential rights: 1. exclusively right to use that product. 2. To obtain relief from the infringement of the product. 3. Right to assign the TM in consideration to use. The right in the trademark are confer by two ways that is by registering the trademark in registration office i.e. patent and registration office or by being the first one to use that trademark in commerce.

1.11ACTIVITY

Explain the essentials of trademark in cyber spacing along with detailed account on the infringement and its remedy. (Word count- 2000 to 2500).

2

Unit 2: INFRINGEMENT OF TRADEMARK IN CYBER SPACE

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 What is domain name

2.4 Trademark and Domain name

2.5 Dispute between Trademark and Domain name

2.6 Forms of infringement of trademark in cyberspace

- 2.6.1. Cyber Squatting
- 2.6.2. Reverse domain name hacking
- 2.6.3. Meta tabs

2.7 Let's sum up

2.8 Further reading

2.9 Check your progress: Possible Answers

2.10 Activity

2.1 LEARNING OBJECTIVE

After going through the chapter, you should be able to understand the-

- Relevant aspects attached to trademark in relation to domain name.
- Significance of domain name under infringement of trademark
- Different types of infringement under trademark.

2.2INTRODUCTION

Issues of Trademark Law and Domain Names in Cyberspace "A logo capable of being depicted graphically and capable of separating the products or services of one individual from those of another, and may include the form of goods, their wrapping, and combinations of colours," according to the definition of a trademark.[80]

A trademark is used to distinguish the origins of a product's origin. The four purposes of a trademark are as follows:

i. It defines the substance as well as its source.

ii. It maintains the product's consistency.

ii. It promotes the commodity.

iv. It provides a mental picture of the commodity in the public's mind, especially among consumers or potential consumers of such products.[81] Lee, Skoda, Colgate, Pepsi, Brooke Bond, Sony, among other trademarks, are examples.

2.3WHAT IS A DOMAIN NAME?

Simply placed, a domain name is a linguistic equivalent to what we refer to as an IP address. Per machine has a unique identifier, which functions similarly to a phone number. If you wish to contact a friend, you must first dial the friend's phone number. Similarly, if he wants to reach a website, he would type in its IP address. However, because it's difficult to recall a long number like 202.162.227.12, a mechanism has emerged in which a name is translated to the relevant phone number or IP address.

[80] Section 2(1)(zb), The Trademark Act, 1999.

[81] Dr. B.L. Wadhera, Law relating to Intellectual Property, Universal Law Publishing Company, New Delhi, 2009, at pg. no. 134.

As a result, instead of typing 202.162.227.12, one can now simply type www.tata.com.

What exactly does a domain name entail? These unmemorable lines by the great poet William Shakespeare were most certainly composed at a period when patents and domain names were unknown. If Shakespeare had known that Shakespeare.com was for sale, he would have thought twice about writing those words. As a result, the importance of domain names should not be overlooked.[82]

2.4TRADE MARKS AND DOMAIN NAMES

Cyberspace does not constitute a substantive change to ordinary trademark infringement. It may be easier to infringe trademarks on the internet, but the actual infringement is not a qualitatively different phenomenon as such. However, there is one important exception: the conflict between trade marks and domain names which is characteristic of the cyberspace. Trade marks are signs capable of being represented graphically and capable of distinguishing goods or services of one undertaking from those of other undertakings. Domain names are a different and more user-friendly expression of internet protocol addresses (unique numbers that identify each computer linked to the internet) that indicate the location of a given website. The question of infringement arises if a domain name is confusingly similar or identical to a trademark. Very often, this is even intended by the registrant of the domain name. He registers (in bad faith) a domain name that is identical to a known trademark or trade name of a company and then offers that company the domain name against payment of a large sum of money – 'cybersquatting'.

In the UK the principal decision in this regard is BT (and others) v. One in A Million: where there is clear evidence of systematic registration by the appellants of well-known trade names for blocking registrations and for extracting money from the owners of the goodwill in the chosen name, that is a threat to exploit the goodwill by trading under that name. The registering of a distinctive name makes a representation to persons who consult the register that the registrant is connected or associated with the name registered and thus the owner of the goodwill in the name.

[82] S. K. Varma& Mittal, Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, 2003, at pg. no.154.

This amounts to passing off and also to trademark infringement.[83] Usually, conflicts between trademarks and domain names are resolved according to the Uniform Domain Name Dispute Resolution Policy (UDRP), which operates worldwide. The registrant submits to this process on registration of his domain name. Where the registrant's domain name is identical or confusingly similar to the complainant's trademark, the registrant has no legitimate interests in the domain name, and the domain name has been registered and is being used in bad faith, UDRP will cancel, transfer or change the domain name.[84]Although the law on infringement is clear, it is also obvious that in fact, cybersquatting opens up a large field of potential cyberwar activities.

2.5DISPUTE BETWEEN TRADEMARK AND DOMAIN NAMES

The Trademark Act, 1999 has been enacted with an object to amend and consolidate the law relating to trademarks for goods and services and for the prevention of the use of fraudulent marks. However, trademark owners desirous of using their marks as domain names have found that such domain names have been recognized by unauthorized parties, often as a deliberate attempt to violate the rights of the original trademark owner. Actually, domain names are registered on a 'first come, first serve basis' which leads many a time to what are commonly referred to as 'abusive registrations', i.e. registration by a person of a domain name containing a trademark, in which such person/entity has no legitimate right or interest.

2.6FORMS OF INFRINGEMENT OF TRADEMARK THROUGH CYBERSPACE

2.6.1 Cybersquatting:

Various forms of domain name cases are brought to courts around the world. Most of the more extreme forms of lawsuits has been "Cybersquatting," which entails the use

[83] BT (and others) v. One in A Million and others [1999] 1 WLR 903, at 924-926, CA. Discussion of other cases on cyberpiracy in the US and the UK, see Younes (2012: 849-850)

[84] UDRP policy as approved by ICANN (Internet Corporation for Assigned Names and Numbers), http://www.icann.org/en/help/dndr/udrp/policy (visited 7 Feb. 2014), paras. 3, 4(a) and (i).

of a domain name by someone who has not claimed the name nor any intrinsic claim to it. Since trademarks and domain names are identical, certain individuals have taken advantage of this by registering trademarks of others as domain names and then selling such domain names to trademark owners or third parties for a fee. This is referred to as “cybersquatting,” which refers to someone sitting in another person’s house. Cybersquatting is an abusive process in which one party registers a domain name that contains the name or trademarks of another. This activity demonstrates the significance of domain names in defining online identities. This method is well-known in order to either prevent a legal customer from registering their most desired domain name or to sell the names for a profit on the open market. As a result of this cybersquatting pattern, courts are looking into the relationship between trademarks and domain names. To file a cybersquatting suit, the plaintiff must show deception, a violation of legal rights and interests, and a domain name that is identical to the trademark.

2.6.2 Reverse domain name hijacking:

Reverse cybersquatting is another term for it. It arises when a trademark owner seeks to secure a domain name by filing bogus cybersquatting charges against the legitimate owner of the domain name in court. In domain name dispute proceedings, reverse domain name hijacking, or RDNH, happens when a copyright owner tries to secure a domain name by wrongly alleging cybersquatting against the domain name owner.

This differs from domain name hijacking, which is commonly synonymous with cybercrime and involves the theft of a domain name via unauthorized access to the domain management account or domain name system (DNS) hijacking, which involves the modification of a domain’s name servers via similar unauthorized access.

In other words, RDNH occurs when a trademark owner uses UDRP litigation to force an actual domain owner to relinquish their domain name rights. This strategy is against the law, which explicitly indicates that the claimant must certify that they are not exploiting the procedure to intimidate a domain holder and that they are behaving in good conscience through fair arguments. Domain name owners are often forced to sell ownership of their domain names to trademark owners in order to escape court litigation and expensive costs, particularly where the domain names belong to smaller businesses or individuals who are unable to afford to contest the lawsuit.

Larger companies and well-known affluent people are the most prominent perpetrators of reverse domain name hijacking.

- **What can companies do to avoid attempted RDNH?**

There is an increased chance of the respondent requesting an RDNH decision where the trademark is made up of common terms or where the domain name has no substance. Trademark owners who have ample reasons or who do not act in poor conscience will avoid an RDNH decision.

Recommendation to trademark owners:

- Make sure the trademark or rights predate the last registrant's domain name registration or purchase (in case a domain name has changed hands). It would be impossible to argue "bad faith" if prior rights cannot be confirmed, since the UDRP hinges on registration and usage.
- Document how well the trademark was known at the time the contested domain name was registered; whether the domain name is 20 years old, how well it is known today is meaningless.
- Claims that are backed up with proof. Present no allegations of your favour or try to dismiss the respondent without evidence.
- Be truthful with the jury. If you tried to purchase the domain name from the registrant before filing the UDRP, tell us about it. No tribunal would hold a complainant responsible for attempting to reclaim a domain name more easily or cheaply than via the UDRP, although they would remain unimpressed whether the complainant claims the respondent attempted to market the domain name to them at an unfair price since the complainant initiated the conversation.
- Avoid overt efforts to entrap the respondent or deceive the jury, such as submitting only partial material information, the particulars of which are revealed when the registrant files their answer.
- Finally, think about who and who you'll turn to if you have a disagreement. Without proper analysis of the evidence, a boilerplate solution avoids leaving the trademark owner vulnerable to not only a loss but also the presumption of underhanded tactics.

2.6.3 Meta tags:

Meta tags, also known as Meta elements, are a type of web page feature. Meta tags include details such as website titles, keywords, and other pertinent material. Meta tags were originally used in search engines to describe what a website was for a while the internet was in its infancy. Meta tags were also used to help position web sites in the relevant categories. People nowadays use Meta tags to generate fake page rankings for badly designed web pages. Meta tags are classified into three categories: title, definition, and keywords.

Meta tags are divided into two categories: context meta tags and keyword meta tags. The context meta tag, for example, includes a brief summary of the website. The keyword meta tag, on the other hand, is a word or phrase that best defines the website's subject. Other useful meta tags, such as the meta http-equiv tag, the meta reset tag, the meta copyright tag, and the meta author tag, provide additional information to web browsers and search engines.

The use of a third-party trademark in one's meta tags is the key point of controversy when it comes to meta tags. To draw Internet traffic, website owners, for example, add third-party trademarks in meta tag info. This will cause traffic to be diverted away from the trademark owner's website. Misuse of meta tags can enable the website owner to benefit from public attention and sales that are misdirected. Intentional trademark infringement can occur when website operators use third-party trademarks in meta tags, website copy, and code meta tags.

2.6.4 Loopholes under the IT, Trademark

In India's new or proposed Information Technology Act, there is no clause to jail cyber-squatters; at most, the domain can be taken back. Despite the fact that the IT Act does not provide for civil compensation, To discourage squatters from grabbing more domains, the IN Registry has taken aggressive measures to reward victims. The majority of squatters, on the other hand, go by aliases. The National Internet Exchange of India (NIXI) is a. IN Registry is a self-contained entity that is primarily responsible for the upkeep of the. IN cc-TLD (country code top-level domain), as well as maintaining its organizational continuity, reliability, and security. It will carry out the different aspects of the current strategy outlined by the Indian government's Ministry of Communications and Information Technology's Department of Information Technology. The Information Technology Act is defective in certain areas, such as authority, cybercrimes involving IPR, cyber harassment, cyber slander, and so on.

Similarly, the Indian Trademark Act, 1999, is vague on questions resulting from trademark violations on the internet.

2.7LET'S SUM UP

In this chapter, we have analyzed the concept of cyberspace in light of trademark infringement. In addition to that, we understood the various type of trademark infringement in cyberspace and how domain name id studies in the given context. Besides, we have also learned about the loopholes under trademark legislation.

2.8FURTHER READING

- Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publications, Edition 4th, 2011
- Dr. GeorgiosZekos, Issues of Cyberspace and E-Commerce, ICFAI University Press, 2008
- Dr. Gupta & Agarwal, Cyber Laws, Premier Publishing Company, Allahabad, 2010 • G.D. Khosla, Know Your Copyright, Eastern Law House Publication, Calcutta, 1986
- Harish Chander, Cyber Laws and IT Protection, PHI learning Private Ltd. Publication, New Delhi, 2012 RohasNagpal, Intellectual Property Issues and Cyberspace, Asian School of Cyber Law Publication,Pune,2008
- S. K. Varma& Mittal, Legal Dimensions of Cyberspace, Indian Law Institute, New Delhi, 2003
- V.K. Ahuja, Intellectual Property Rights in India, Lexis Nexis Butterworth's Wadhwa, Nagpur, 2009 VakulSharma, Information Technology, Universal Law Publishing Company, New Delhi, 2013.

2.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is a domain name?

Domain name is the linguistic counterpart of what we call an Internet Protocol address. Every computer has an address, which is akin to a telephone number.

2. Define Mega Tags.

Meta tag is an element of web pages that are also known as Meta elements. Meta tags provide information about page descriptions, keywords and other relevant data.

3. Explain the reverse domain name hacking.

It is also known as reverse cybersquatting. It happens when a trademark owner tries to secure a domain name by making false cybersquatting claims against a domain name's rightful owner through legal action.

2.10 ACTIVITY

Provide a detailed account of the domain name along with different types of trademark infringement. (word count 2000-2500)

Unit 3: TRADEMARK LAW IN CYBERSPACE: PROTECTION TO INTERNET ADDRESS

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Disputes relating to Trademark in Internet Domain Name

- 3.3.1 Cyber Squatting
- 3.3.2 Reverse Domain Name Hijacking
- 3.3.3 Typo-Squatting

3.4 Relation of Dispute Resolving between UDRP and the Courts

3.5 Position in India

3.6 Let's sum up

3.7 Further reading

3.8 Check your progress: Possible Answers

3.9 Activity

3.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- How UDRP (Uniform Dispute Resolution Policy) deals with the same situation at an extra-territorial level.
- The legal position under trademark law for protection of trademark in cyberspace
- Some suggestions as to how Indian Trademark Laws can make the working of UDRP better by working on its own laws.

3.2INTRODUCTION

The history of trademark law to the cyberspace can be associated with the creation of the World Wide Web (www) which certainly created a link of trademark law with Internet domain name disputes. It has also sparked interest among consumers as a means of commercializing the Internet medium. Thousands of companies have created online storefronts to distribute publicity materials, provide customer support, and sell merchandise and services. As a result of this commercialization aspect, trademark law and domain name law are being increasingly intertwined. Consequently, the following dynamic growth of the World Wide Web has issued new challenges to the intellectual property consultants concerning trademark infringement.

For trademark owners, internet is a profitable platform, but in certain cases, it turns out to be problematic in their business growth. These trademark owners often have to deal with certain domain name disputes inflicted by the third party like cybersquatting etc but in India, we per say do not have any Domain Name Protection Law so the cases relating to cybersquatting are decided under Trade Mark Act, 1999.[85]

Under the current law, section 29 provides for the protection of registered trademark and the protection for unregistered trademark has been provided in section 32. However, the act is silent on the protection for trademarks infringement in the cyberspace. The bulk of domain name cases appear to include trademarks, as it is said that the conflict stems from the ownership or use of the domain name infringing

[85] See generally Gary W. Hamilton, Trademarks on the Internet: Confusion, Collusion, or Dilution?, 4 TEx. INTEL. PROP. L.J. 1, 2 (1995); Dan L. Burk, Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks, I RICHMOND J.L. & TECH. 1, $ 2 (April 10, 1995) .

with some lawfully recognised right, such as a trademark, a common law privilege of handing off, or some other right.

As trademark laws are territorial in nature but internet in the global domain so the dispute involving bad faith registrations are typically resolved using the UDRP (Uniform Domain Name Dispute Resolution Policy) process which is developed by the ICANN. Under UDRP, WIPO happens to be the leading ICANN accredited domain name dispute resolution service provider which was established as a tool for promoting the protection, dissemination, and the use of intellectual property throughout the world. Since TRIPS agreement provides for only minimum standards so, there exists similarity up to some extent in the domestic IP laws and except these principles there are hardly any laws which are uniform, and as a result of which there exist some advantages and disadvantages of nation over other nations IP laws.[86]

3.3DISPUTES RELATING TO TRADEMARK IN INTERNET DOMAIN NAME

Let's start with the question why do domain names need a legal protection? On one hand, domain names provide great economic value to the online business and on the other, these names are exposed to many ways in which it puts domain names at risk. The risk particularly includes;

3.3.1 Cyber squatting is described as "the registration of a domain name by someone who does not have a legal right to the name with the intent to

(i) sell the name,

(ii) (ii) block the trademark holder from having rights to the name, or

(iii) (iii) divert traffic to a name in the hopes of a trademark owner making a bid for it."

In the case of 'Green Products Co. v Independence Corn By-Products Co.'[87] (ICBP), for example, both firms were rivals in the corncob by-product sector. ICBP

[86] Robert J. Raskopf, Trademarks and the Internet, in INTELLECTUAL PROPERTY LAW INSTITUTE 1047 (Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G-416, 1995). For a description of how domain names are created and assigned, see infra Part III.

[87] 992 F. Supp. 1070

licensed the domain name (greenproducts.com) but has yet to create a website. The court determined that ICBP's goal was to use its confusing domain name to attract new users to the site after it was launched, and that it sought to profit unfairly from the use of Green Product's name. Consumers may not be confused after visiting the site, but they may only purchase the product from the ICBP's site, according to the court. The court ruled that it was violation based on these results.

3.3.2 Reverse Domain Name Hijacking; as people file confusingly identical domain names, they point them to gripe pages that contain some propaganda.

3.3.3 Typo-Squatting; done by people who register the domain names incorporating variations of well-known trademarks terms such as misspellings (micr0soft.com) or adding of prefixes or suffixes to the existing domain name (yahooindia.com) and use them for websites to take advantage of unwary Internetusers.

Yahoo Inc. Corporation v Akash Arora[88] is the first case in which the Indian Court that discussed the issues revolving services offered through the Internet. The plaintiff, in this case, submittedthattheyhadtheregistrationofthedomainnameyahoo.comwithNetworkSolutions Inc.andhadregistrationsofthesameinmorethan69countries.Thedefendantcontended that he had provided a disclaimer in his website which avoided the confusion, also, that yahoo is a dictionary word and could not be protected but the High Court of Delhi held that the marks were similar and disclaimer does not help as people still would associate it with the original yahoo, administratively or economically. Furthermore the word yahoo was protected as it was a well known trademark used by the Plaintiff and wasdistinctive.

The main problem regarding this dispute arises with Cyber Twinswhich occurs when both thedomainnameholderandthechallengerhavealegitimateclaimtoadomainnamethent hey are known as cyber twins. The cases involving cyber twins are the most difficult to be resolved, because, the law of trademark and unfair competition may otherwise allow both parties to enjoy concurrent use of both. Both types of

[88] 1999 Arb. L. R. 620

conflicts may occur on two levels: first, when the same mark is owned and used by different people for different types of goods or services; and second, when the same mark is used and used by different people for different types of goods or services. Second, 'territoriality' occurs where the same symbol is owned and used by different people in different countries in relation to the same products or services.

Both companies have a legal claim to the domain name (dci.com) in ***Data Concepts, Inc. v Digital Consulting Inc.***[89] and both of them had patent rights for DCI. Data Concepts, on the other hand, licensed the domain name dci.com in 1993.It would seem that, in the cases where both have claims then the entity first to register would get it but The Sixth Circuit ruled that there still was possibility of infringement. Since trademark infringement is both a reality and a legal issue, the case must proceed through a full trial before an infringement decision can be made. Owing to a lack of documentation and the fact that Digital was unaware of Data's previous life, the lawsuit was dropped when Data did not show that dci.com was misleading people between the two tags.

3.4RELATION OF DISPUTE RESOLVING BETWEEN UDRP AND THE COURTS

The UDRP applies to second-level domain name registrations in the following 14 generic top-level domains (gTLDs):

.aero,.asia,.biz,.cat,.com,.coop,.info,.jobs,.mobi,.museum,.name,.net,.org,.pro,.tel, and fly. However, some of the above-mentioned gTLDs are only covered by rules and procedures rather than the UDRP. For example, in the.name room, there are two dispute resolution policies that may be applicable to second-level domain name registrations: the UDRP and the Eligibility Requirements Dispute Resolution Policy (ERDRP), both of which are seldom used by Indian registrants. A claimant must define the following three elements to succeed under the UDRP:

(i) "Because the domain name is identical or confusingly similar to a

[89] 150 F.3d 620

complainant's trademark or service mark;

(ii) That the registrant has no ownership or legal privileges in the domain name; and

(iii) That the registrant registered and used the name in bad faith."

The process of getting redressed under UDRP is conducted online with a single electronicand hard copy document submission of facts and legal arguments which makes the process simple and easily accessible. Service of process can be achieved by email to the address in the registrar's record. Under the rules of UDRP, the panelists take their decisions on whichever law they think as fit in a particularcase.

Butdespiteitsobviousachievement,lackoforaltestimonyandrulesofevidenceinthesepaper proceeding makes it difficult to evaluate the disputed facts and ascertain the credibility of the evidence produced. Panelists deliver the judgment only on the evidences produced in front of them, so they have to regard that as reliable where there is lack of documentary evidenceeven inthecasesoflegitimateinterest.Soisitnotnecessarythatsameorrightconclusionisreached in this type of Resolution Policy as the decision in UDRP or courts would differ according to where better evidences are put forth. Moreover the decision of the UDRP is not binding on thecourtsoflandwhichsometimesturntobedefeatingtheveryinitiationofdecisionbyUDRP

andthetrademarkownersarethevictimsofsuchthing.Asalsoseen,inthecaseof***Referee Enterprises Inc. v Planet Ref. Inc.,***[90]where the dispute was between the magazine publisher and another publisher on online medium, the plaintiff initiate the UDRP proceedings in the basis of his ownership on the term referee as hid magazine title, challenging his rivals mark "ereferee" on domain name, the panel negated the complaint on the ground that the wordused by the plaintiff is the word which is generic in nature the publisher subsequently filed thecase against the inferior alleging him violating the federal trademark law, the court in response granted the preliminary injunction which was broad to the extent that it prohibited the defendant to use all the domain names having the word in dispute court did not

[90]2001 U.S. Dist. LEXIS 9303

take thenotice of UDRP proceedings and did not mention the decision in its ruling. Furthermore in a case where the applicant brought the subsequent suit in the court after being defeated in the UDRP proceedings, the trademark owner moved to dismiss the action on the grounds that it do not have sufficient grounds to vacate arbitral award of UDRP, the court denied this argument by saying that Federal Arbitration Act do not applies to the UDRPproceedings.

The case ***Maruti.com et al. v. MarutiUdyog Ltd. et al.,***[91] where MarutiUdyog, an Indian company with a well-known name in India, has already registered marutiudyog.com as its domain name in the United States, is one of several cases of the system failing. The domain name "maruti.com" was obtained by the respondent. When the appellant filed a lawsuit with the WIPO, the panel ruled in favor of Udyog. In addition, the respondent has been labeled a cyber squatter by the WIPO panel three times in WIPO arbitration cases brought by Onida, Hero Honda, and Maruti. However, when the matter was brought to the US courts, the WIPO panel's rulings were deemed non-binding. Even the Anti-Cybersquatting Consumer Protection Act of the United States was said not to apply. The court ruled that since Maruti did not make or market cars in the United States, it was not entitled to trademark rights under the Lanham Act of 1946.

3.5POSITION IN INDIA

Another question that needs to be resolved is whether or not the country's trademark laws are sufficient to remedy the situation.

The court in the case of ***Satyam Infoway Ltd v. Sifynet Solutions (P) Ltd***,[92] which was decided in 2004, nailed the Indian domain name situation, citing that-

"As far as India is concerned, there is no law that specifically applies to domain name dispute resolution. While the Trade Marks Act of 1999 is not extraterritorial in nature and does not have appropriate safeguards for domain names, this does not preclude domain names from being lawfully covered to the degree practicable under passing off laws."

[91] 447 F. Supp. 2d 494 (D. Md. 2006)
[92] 2004(3)AWC 2366 SC

In India, since, there exists no direct law to wrestle the threat of such disputes; hence courts have largely used the principle of passing-off.

Despite the fact that the national court system is not constrained by the WIPO Arbitration Panel's ruling, they have made numerous judgments and judicial decisions based on the ICANN's UDRP Policy, demonstrating that the courts consider the UDRP's policies and decisions to be of sound authority on the subject.Oneoftheexamples demonstratingthesameis***ManishVijv.IndraChugh,***[93]inthiscase,With the copyright and domain name "www.kabadibazaar.com," the appellant was selling secondhand goods on the internet. Within a month of plaintiff's launch, defendant launched "www.kabarribazaar.com," claiming a larger media profile than plaintiff. The complainant filed a complaint with the WIPO Uniform Dispute Resolution Policy, 1999, alleging that the defendants registered the domain name "www.kabaribazaar.com" with a malicious intent. The panel held that it was not possible to prove that the registration of the domain name was in a bad faith as “Kabadi- bazaar” is a common term in the hindi language and so the plaintiffs domain name had not acquireda secondary meaning. It also referred to the Rules 4 (a) and 4 (b), found that both parties had operatedtheirwebsiteswithinamonthandwhiletheplaintiffwasunabletoshowthequantum ofbusinesscarriedout,itcan’tbesaidthatthedefendanthadnotincurredadvertisementcosts. Therefore, it dismissed the plaintiff’s application and vacated the interim injunction order against thedefendant.

This, thus, can be said that the national courts can easily shift domain name cases towards ICANN’s UDRP mechanism which is an efficient alternate dispute resolution remedy easing the over burdened domestic court system of a country.

It is of no argument that UDRP has been proved to be the simplified and cost friendly way of getting justice over the issue of domain name disputes to tackle the online disputes affecting the landmark owners in an era of online world but a lot is still to be done to make it a better working at the territorial level. The global experience has shown that many other countries have even tried to plug the legal

[93] AIR 2002 Delhi 243

lacuna by passing separate law for dealing with the problem like US has passed Trademark Cyber Piracy Prevention Act, 1999. Likewise, India also needs alawregardingthesamesincebringingthepassinglawprincipledoesnotprovideforanenti re solution to the issue in question. There should be a provision for easier and supplemental methodofregisterforeachStateundertheIndiantrademarklawsothattheownerwhowant s a territorial registration only does not have to be tortured with 'n' number of procedural formalitiesduetowhichalotoftimecanalsobesaved.Theperiodofnon-useofatrademark forfiveyearsasagroundforrevocationshouldbereducedtothree yearsunderthe Indianlaw so that one does not take advantage of getting a name registered from stopping some other squatter to use the same as they know how tedious and lengthy the process of litigation is. Another suggestion is that there should be a provision regulation of cyber crimes especially cyber squatting, not only under trade mark law but also in Information and Technology law in order to protect the rights of the legitimate claimers at territorial as well as extra-territorial level.

3.6LET'S SUM UP

In this chapter, we have learned legal position under trademark law for protection of trademark in cyberspace. The chapter also discusses the issue of inadequacy of laws for dealing with this matter. It further outlines as to how UDRP (Uniform Dispute Resolution Policy) deals with the same situation at an extra-territorial level according to the mechanism provided by ICANN (The Internet Corporation for Assigned Names and Numbers). Finally, we learned about some suggestions as to how Indian Trademark Laws can make the working of UDRP better by working on its own laws.

3.7FURTHER READING

- WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP); WIPO; Date of Access: 24.10.2019 <https://www.wipo.int/amc/en/domains/guide/>
- Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886); WIPO; Date of Access:

24.10.2019< https://www.wipo.int/treaties/en/ip/berne/summary_berne.html>

- Summary of the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (1961); WIPO; Date of Access: 24.10.2019 <https://www.wipo.int/treaties/en/ip/rome/summary_rome.html>
- Aurélie Pols, Ewa Bałazińska, Karolina Lubowicka: OECD Guidelines: 8 Privacy Principles to Live By; PiwikPro Dated: 21.09.2018; Date of Access: 24.10.2019 < https://piwik.pro/blog/oecd-guidelines-8-privacy-principles-to-live-by/>
- Linking, Framing, Meta Tags, and Caching; Date of Access: 24.10.2019 < https://cyber.harvard.edu/property00/metatags/main.html>
- Linking, Framing, and Inlining by Richard Stim; Nolo; Date of Access: 24.10.2019 < https://www.nolo.com/legal-encyclopedia/linking-framing-inlining-30090.html>

3.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the elements to establish the complaint under UDRP?

A claimant must define the following three elements to succeed under the UDRP:

(i) "Because the domain name is identical or confusingly similar to a complainant's trademark or service mark;

(ii) That the registrant has no ownership or legal privileges in the domain name; and

(iii) That the registrant registered and used the name in bad faith."

2. Provide the provisions for trademark protection.

Under the current law, section 29 provides for the protection of registered trademark and the protection for unregistered trademark has been provided in section 32.

However, the act is silent on the protection for trademarks infringement in the cyberspace.

3.9 ACTIVITY

Discusses the legal position under trademark law for protection of trademark in cyberspace. (Word count 2000-2500)

4

Unit 4: DOMAIN NAMES, THE INTERNET, AND TRADEMARKS

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Internet domain name and trademark infringement

4.4 Judicial Pronouncements

4.5 Should domain name be protected as trademark

4.6 Special challenges to traditional trademark law post by domain name registration on the internet

4.7 Let's sum up

4.8 Further reading

4.9 Check your progress: Possible Answers

4.10 Activity

4.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- The unique problems that conventional trademark law faces as applied on the Internet.
- The controversy on trademarks and domain names is addressed by assessing the benefits and limitations of the InterNIC regulation on domain name registration.
- Possible solutions offered on domain names.

4.2INTRODUCTION

Law academics have spent the past few years examining how digital data transfer over the Internet - the world's largest computing network - has questioned and tested existing legal principles and doctrines, especially in the field of intellectual property. For those attempting to preserve the goodwill and intrinsic meaning encapsulated in a trademark, the Internet presents special challenges. The alleged violation of established trademark rights by computer users who register allegedly infringing domain names, or computer addresses, will be addressed in this chapter, as will the settlement of conflicts between two would-be users with legal claims to the same domain name.[94]

The Internet is a global network of interconnected data networks that connects

[94] See generally Gary W. Hamilton, Trademarks on the Internet: Confusion, Collusion, or Dilution?, 4 TEx. INTEL. PROP. L.J. 1, 2 (1995); Dan L. Burk, Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks, I RICHMOND J.L. & TECH. 1, $ 2 (April 10, 1995) .

millions of users and enables them to exchange and transmit resources and information. There is no single government that controls or regulates the Internet. As a result, "there is no central body to control Internet access, no one to ask for permission to enter the network, and no one to report to when things go wrong" since each machine connecting to the Internet operates autonomously and is only supervised by its own systems administrator. The United States Department of Defense created the Internet to link geographically distributed scholars.

The Internet, on the other hand, now links millions of people around the world, provides a high-speed, reliable, and effective networking network by which people can access, exchange, and distribute a vast array of information and services.

In recent years, commercial use of the Internet has accelerated, converting the network infrastructure from a testing instrument to a digital marketplace capable of serving millions of consumers worldwide. ' As a result, many businesses have positioned themselves to sell their products and services over the Internet in order to tap into a demand of 30 million potential customers. Just 30,000 businesses used the Internet in December 1994, but by February 1996, 175,000 businesses had a kind of online presence. By January 1996, over 300,000 people and businesses had created home pages on the World Wide Web, a branch of the Internet that offers a hypertext-based distributed information system that allows users to build, search, and delete hypertext records.[95] This burst of activity has rapidly transformed the Internet from the "cozy, non-commercial atmosphere"' that marked its early years to a platform for commercial retailers to advertise, market goods and services, distribute software and other devices, and provide on-line services.

4.3INTERNET DOMAIN NAMES AND TRADEMARK INFRINGEMENT

A. What is a Domain Name?

Other users must be able to identify and find each device or user connecting to the Internet. As a result, each user is given an Internet Protocol Address (IP

[95]Thomas K. Thomas, NIXI To be Registrar for .in Domain Name, October 27, 2004, *available at*http://www.thehindubusinessline.com/2004/10/27/stories/2004102701720700.htm

Address), which is a specific string of numbers separated by intervals that represents various fields, such as 123.101.23.128. A network component of these strings of digits identifies the particular network to which the user is associated, while a local address identifies the user within the network. Unfortunately, IP addresses are unwieldy and difficult to remember. As a result, the IP Address system has been replaced by a more user-friendly domain name system, in which IP Address holders are given a mnemonic designation that is easy to recall. The numeric IP address that corresponds to the designated mnemonic domain name address is automatically looked up by computer programs that link users to the Internet.[96]

To designate fields, domain names are made up of a series of characters divided by intervals. A term that can readily distinguish the holder of the address, such as an individual's or company's name, a brand name or trademark, or a nickname, is often used in domain names, accompanied by a three-letter abbreviation that designates the user's form of organization.

B. Trademark Skirmishes on the Internet

The commercialization of the Internet has resulted in a series of legal battles between trademark owners and Internet users that have registered domain names that could infringe on the trademark owners' rights. These conflicts clearly demonstrate the conflicting interests at stake and the kinds of controversy that the domain name registry system has sparked.

4.4JUDICIAL PRONOUNCEMENTS

1. MTV v. Adam Curry[97]

MTV Networks (MTV) sued Adam Curry, one of its former video disc jockeys, in October 1994, claiming copyright infringement in connection with Curry's use of the domain name "mtv.com" to find his Internet portal. To decide who had legal rights to

[96]Eric Misterovich, Domain Names as Registered Trademarks, *available at* https://revisionlegal.com/trademark-attorney/domain-names-as-registered-trademarks/
[97]867 F. Supp. 202

use the logo, the two sides went to court in the Southern District of New York. Curry said that he was granted permission to use the name when working with the network to create an Internet portal that disseminated regular coverage of film and music industry gossip. Curry registered the domain name "mtv.com" under his own name and paid for it with his own money, and he continued to publish regular updates from the site long after his employment at MTV ended. Curry's website was very popular, with millions of visitors in the first ten months of its existence.

MTV sued Curry for copyright violation and violation of his work contract after many failed demands that he stop using the "mtv.com" brand for his website. Despite Curry's promise to take the case "all the way to the Supreme Court" and his description of the case as the "Roe v. Wade of the Internet and the technology superhighway,"84 the case was never resolved in district court. Curry relinquished the "mtv.com" domain name to MTV on unspecified terms in March 1995, and the two sides settled their disagreement. Nonetheless, the significance of this case was undeniable; it was one of the first, and most well-known, 85 efforts to resolve the risk of patent infringement in cyberspace.

2. Stanley Kaplan v. Princeton Review[98]

Stanley Kaplan and Princeton Review, two competing test-preparation firms, decided to arbitrate the first publicly known instance of "Internet address poaching and speculation," the crime of hoarding lucrative trademarked names for use as Internet addresses and keeping them for ransom, in October 1994. In May 1994, Stanley Kaplan applied to trademark the domain name "kaplan.com" in order to create an Internet portal to promote its services, only to discover that the name had already been taken by its biggest rival, the Princeton Review.

Although the Princeton Review's president argued that the domain "kaplan.com" was registered solely to "mock and harass" Stanley Kaplan, the name poaching had the potential to harm Stanley Kaplan's company. "Electronic materials disparaging the consistency of Kaplan Review's offerings and extolling the competitive benefits of the Princeton Review courses" were presented to users who accessed Princeton Review's "kaplan.com" platform. Furthermore, users were not informed that the platform was operated by Princeton Review rather than Stanley Kaplan, raising the

[98] https://crushthegretest.com/kaplan-vs-princeton-review-gre/

risk of users being misled about the true source of the information shared on the Internet site.

3. WIRED v. Wire

Wired magazine was pitted against WIRE, a computer network that used the domain name wire.net, in a trademark/domain name battle that focused on a related issue: the registration of a domain name that was identical to one already in use. About the fact that the two organizations provided very different content - Wired is a monthly newsletter that discusses information technology-related subjects, and WIRE is a computer network dedicated to women's issues". Wired felt WIRE's domain name, wired.com, was too close to its own. Despite the fact that both parties retained attorneys to handle the dispute, the parties reached an agreement in February 1994 without having to go to court. Wired promised to share the expense of changing WIRE's name to Women's Wire and ran some advertisements for the network, which even updated its Internet address to wwire.net.

Despite the fact that the case was settled amicably, it posed a question not answered in the trademark/domain name dispute: whether the registry of competing domain names created such a risk of misunderstanding that one of the names needed to be modified.

4.5SHOULD DOMAIN NAMES BE PROTECTED AS TRADEMARKS?

As previously stated, some researchers argue that domain names are not the same as trademarks and thus should not be considered infringing on existing trademarks. They contend that domain names are not entitled to immunity since they are similar to emails. Others, on the other hand, have emphasized that domain names serve the same function as trademarks: they designate the source of the product, service, or material being sold over the Internet, and they enable businesses to move their brand identity and goodwill to the computer network medium. "Domain names will seem odd because they appear to be both names and addresses; they both locate and recognize Internet resources," according to the report. If trademark law only recognized a domain name's ability to find an Internet location, "application of

trademark law to domain names... may be problematic." The second essence of domain names, though, must be considered: their ability to convey the source's identity. Domain names should be protected as trademarks and accepted as worthy of infringement on other trademarks when they have such a valuable purpose of identifying the origins of a product or service.[99]

Critics also claim that the new Internet address scheme is rigid and blinkered, since all business entities are clustered together under the "com" top-level domain identifier. "The.com top-level domain has become insufficient to satisfy the demand for domain names from commercial organizations with related or equivalent names as the Internet has become more commercial," says the study.

4.6SPECIAL CHALLENGES TO TRADITIONAL TRADEMARK LAW POSED BY DOMAIN NAME REGISTRATION ON THE INTERNET

This chapter has already discussed how domain names can be licensed under trademark law and how domain names can be considered potentially infringing on existing trademarks. However, there are certain quirks in the way domain names are used on the Internet that should be taken into account when determining how to handle domain names and trademark violations.

A. Geographic Overlap in Cyberspace

Traditional trademark law states that two firms can use the same trademark as long as their brands or local markets are sufficiently different to guarantee that there is no chance of misunderstanding. As a result, Domino's Pizza and Domino's Sugar will coexist peacefully—and legally—because it's extremely doubtful that a customer would mix up the two brands' origins. Similarly, the Acme hardware store in Lewiston, Maine, and the Acme hardware store in Portland, Oregon, can also legitimately own the name "Acme" because their local markets are sufficiently distinct to eliminate the possibility of confusion. However, since the Internet is simply one vast geographic region, one domain name cannot be given to two individuals or businesses, regardless of how different their goods or markets are.

[99]Wipo Cyber Squatting Cases Hit record, *available at*http://www.wipo.int/pressroom/en/articles/2017/article_0003.html

In cyberspace, there are no realistic barriers that cause two businesses of the same name to coexist peacefully and profitably. Moreover, ""Usage of domain names that act as popular logos of more than one corporation will become more difficult as businesses continue to use their [Internet] presence to enable consumers to purchase goods," as companies begin to use their [Internet] presence to allow customers to order products. When two entities claim the same trademark under the current rules, "Even though the other side has been using the logo on which it is based for several more years, the first to file may be entitled to keep the domain name. The limitations faced by domain name registrations are obvious in cyberspace, where local markets that are easily distinguishable in "real space" converge and combine.

B. Technological Limitations on the Internet

Domain name addresses are limited to 26 characters due to Internet technical restrictions. "From a 'user-friendly' standpoint, businesses looking to trademark their domain names have an opportunity - and InterNIC encourages - to make them considerably shorter than 24 characters," says InterNIC. As a result, businesses tend to file acronyms rather than their full names, increasing the likelihood that a given name would be sought by other businesses. Companies who formerly coexisted in the industry under separate names but with the same acronym now face the possibility of any legal owner with the same acronym filing the domain name first.

4.7LET'S SUM UP

In this chapter, we have learned legal position under trademark law for protection of trademark in cyberspace and its relationship with domain name. We also aalysed the judicial pronouncements along with relevant legal provisions.

4.8FURTHER READING

- Blake T. Bilstad, Obscenity and Indecency in a Digital Age: The Legal and Political Implications of Cybersmut, Virtual Pornography, and the Communications Decency Act of 1996, 13 SANTA CLARA COMPUTER &

HIGH TECH. L. J. 321 (1997).

- William A. Hodkowski, The Future of Internet Security: How New Technologies will Shape the Internet and Affect the Law, 13 SANTA CLARA COMPUTER & HIGH TECH. L. J. 217 (1997).
- Jo-Ann M. Adams, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 SANTA CLARA COMPUTER & HIGH TECH. L. J. 403 (1996).
- Michael P. Roch, Filling the Void of Data Protection in the United States: Following the European Example, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 71 (1996).
- Joshua D. Blackman, A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 431 (1993).
- Halina S. Dziewit et al, The Quest for the Paperless OfficeElectronic Contracting: State of the Art Possibility but Legal Impossibility?, 5 SANTA CLARA COMPUTER & HIGH TECH. L. J. 75 (1989).

4.9CHECK YOUR PROGRESS:POSSIBLE ANSWERS

1. **What is a Domain Name?**

Other users must be able to identify and find each device or user connecting to the Internet. As a result, each user is given an Internet Protocol Address (IP Address), which is a specific string of numbers separated by intervals that represents various fields, such as 123.101.23.128. A network component of these strings of digits identifies the particular network to which the user is associated, while a local address identifies the user within the network.

4.10 ACTIVITY

Write a detailed note on special challenges to traditional trademark law posed by domain name registration on the internet. (Word count 2000 to 2500)

Block-4

EMERGING ISSUES IN RELATION TO IPR AND CYBERSPACE

Unit 1: IPR MANAGEMENT: EMERGING CYBERSPACE ISSUES IN KNOWLEDGE SOCIETY: A CRITICAL ANALYSIS

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Rationale for Intellectual Property Rights

1.4 Digital Environment and Copyright

1.5 Internet and Intellectual Property Rights

1.6 Protection of Computer Software: The Existing Regime

1.7 Indian Scenario

1.8 Piracy in the Digital Era

1.9 Let's Sum Up

1.10 Further reading

1.11 Check your progress: Possible Answers

1.12 Activity

1.1 LEARNING OBJECTIVE

In this chapter, we will learn:

- Dangers to financial and commercial transactions
- Global standards on electronic crime

1.2 INTRODUCTION

Inventions, literary and artistic creations, and marks, titles, pictures, and patterns used in commerce are all examples of intellectual property (IP) rights granted by society to persons or organisations. For a limited time, they grant the developer the freedom to prohibit anyone from allowing illegal use of their land. Industrial Property (commercial innovations) and Artistic and Literary Property are two types of intellectual property (cultural creations). Current technical advancements are blurring this line, resulting in the emergence of hybrid sui generis systems.[100] The industrial revolution carried with it its own collection of rules governing industry and economic practice, as well as post-industrial society government. The industrial revolution impacted many areas of the world, leaving former colonies behind, and the legal institutions of so-called developed countries were unable to meet the challenges of industrialization. Meanwhile, the ICR has swept the globe, shattering economic and political walls and undermining existing rules of the developed world. Most emerging countries must make a quantum leap in legal development in order to build capacities to defend national interests and prevent abuse by those who own technologies whose boundaries are uncertain. The invention of the Internet Information Highway and Cyberspace has created a challenge for the world today.

1.3RATIONALE FOR INTELLECTUAL PROPERTY RIGHTS

IPR rationale can be divided into two categories:

- philosophical and
- pragmatic approaches.

[100] Richard, D, (2004), Intellectual Property Rights and Global Capitalism: The political Economy of the TRIPs Agreement, 27 (New York: M.E. Sharpe, 2004)

There is no adequate theory of legal scholarship that establishes the basis of intellectual property rights (IPRs). In the light of rapid technical advancements and growing rivalry within industries, legal scholars' theories, such as economic opportunity reasoning, may be considered contradictory. The European Court of Justice's latest ruling against Microsoft urges a reconsideration of the fundamental precept governing IPRs.

Philosophical approaches are well known in the tradition of British philosophers John Locke (1632-1704), Thomas Hobbes (1588-1679), and Georg Wilhelm Friedrich Hegal of the 18th century (1770-1831). John Locke is a model property as right theorist. According to Locke, property rights, as all rights, are derived from the fact that God gave the world to all humans in general, so how can any one individual possess an exclusive property right in the worldly subject? Locke's solution is brilliant, and it brings one to the concept of private property rights. Locke accomplishes this demonstration by distinguishing between the Creator's collective property and the individual's acquisition of the property.[101]

Hegal's insistence on land ownership as a symbol of freedom led to a different philosophical attitude to intellectual property. George Wilhelm Friedrich Hegel was a German philosopher. 1770 – 1831 Individuals will create and realize their full human identities thanks to property tradition. It has been widely suggested that intellectual property should be unalienable based on this approach. In the light of natural rights and moral rationales, a fundamental point against IPRs is that scientific innovations are largely a social production of collective, cumulative, and interrelated work to which we all contribute, and thus no single individual or company should be entitled to assert the land.

Jeremy Bentham (1748-1832), Adam Smith (1723-1790), Jean Baptiste Say (1767-1832), John Stuart Mill (1806-1873), and John Bates Clark all advocated a pragmatic approach (1847-1938). The fundamental argument of these classical economists is that IPRs offer "the promise of reward," which promotes innovative and technical progress by increasing motivation to discover, invest in, and create new ideas, and without which the innovation inducement will be undermined. The

[101]Hegal, G (2006), The Phenomenology of Mind (1806), available at http://www.marxists.org/reference /archieve/hegal/help/hegelbio.htm

reasoning is that doing research and development and getting an innovation to market can be a long and costly operation with little promise of success at the end of the tunnel.[102]

Patents have been seen to have a positive effect on the economy in a number of surveys. Patent acquisition has been shown to improve the pace of innovation in sectors that depend on patents for intellectual property rights, such as pharmaceuticals and chemicals. Simon Rose discovered a strong statistical association between patents filed and GDP, as well as a similar correlation between patents adjudicated and patents adjudicated. It has been found that after a period of animosity, the number of patent applications in technical innovation declined, having a negative effect on the economy. When appellate courts supported patents, however, the number of patent applications rose, which had a favorable effect on the economy.

IPR-induced incentives to innovate reasoning for the IPR scheme is based on two assumptions:

- Without effective incentives, not enough discoveries can be made. In other words, neither innovation nor manipulation of inventors can occur because capitalists expect that they can generate wealth, making it worthwhile for them to invest their time and resources.
- IPRs are the quickest and most powerful way for society to have both rewards.

According to Robert Merges and Richard Nelson, patents encourage innovation by offering benefits, but once they are liberally approved, other companies are discouraged from engaging in the broad range of follow-on innovative work that enhances or modifies an original invention. They showed how discoveries occur along multi-product trajectories that are cumulative, direction dependent, and dynamic in the sense that each discovery in the pathway is based on one's own or others' current or previous ideas. While there are numerous reasons against patents as a motivator to discover, use, and distribute money more effectively, the traditional

[102] Anderson B (2003), Rational for Intellectual property rights in the Electronic Age, New Economy Handbook (Elsevier Science, 2003).

wisdom by economists, attorneys, and many government officials is strongly skewed in favor of the proposition that protections promote economic development.[103]

1.4 Digital Environment and Copyright

Because of their speed and accessibility, digital technologies have become essential resources for generating and preserving information. Digital intelligence now plays an astoundingly important part in financial markets and in all aspects of everyday life. Copyright law's approach of digital information has been important. The internet, a prominent feature of our day, can better be described as a multimedia way of disseminating information and promoting free speech on a scale never before conceivable. Users interested in gathering resources on a certain topic no longer need to access or preserve physical copies; instead, they may make these records accessible on the Internet (without the author's knowledge) by creating a web document with pointers (hypertext links) to the specified references. The open nature of modern Internet technologies distinguishes it from other traditional forms of communication, allowing users to post to a large audience previously inaccessible due to the limited nature of traditional publication.[104]

1.5INTERNET AND INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights apply on the Internet, but enforcing them is complicated. The cost of reproducing works in digital format is low, and the accuracy of the copies is nearly flawless. Publishers and other copyright holders claim that the Internet harms their intellectual property rights by radically altering the structure and means of publication, leaving their works highly vulnerable to Internet piracy. Because of the Internet's decentralized management, any person can freely disseminate a work on the electronic network known as Cyberspace via any number of networks. A consumer can easily send a job to newsgroups via e-mail or on their personal website.

[103] N.S. Gopalakrishnan, Principles of Intellectual Property, EBC, Lucknow, 2014.
[104] Paul Torremans, Holyoak&Torremans Intellectual Property Law, Oxford Univ.Press, 2010

1.6 PROTECTION OF COMPUTER SOFTWARE:THE EXISTING REGIME

Since the demand for computer programmers and communications applications is rising in size and economic importance, the type of security offered is becoming increasingly relevant. Software is easily replicable and inexpensive to duplicate. It's easy to convert from one programming language to the next. The cost of copying program package for most systems is low in the absence of devices that prevent copying. Even if direct emulation is impossible, resourceful programmers and engineers will often reverse engineer programs.

The law governing intellectual property rights has caused issues with emerging technology, such as computer programmers. The law presumes that everything is either a written work protected by copyright or a computer protected by a patent, but not both at the same time. Data engineers, on the other hand, have both authorship and creativity. As a result of these issues, we are forced to doubt the law's applicability. Sui Generics is seen as an alternative to the intellectual property model, allowing security to be tailored. Legislative intervention or treaty negotiations are needed. Their doctrinal evolution is still taking a long time.

1.7 INDIAN SCENARIO

While the Indian Copyright Act complied with international treaties, the country's new copyright legislation lags well behind that of the West. There is no similar law in India to the US DMCA or EU guideline applying the WIPO Internet Treaties since India did not sign the "WIPO Internet Treaties." The current Indian Copyright Act makes no provision for "technological security mechanisms" or "electronic rights management information" protection. The Indian Penal Code, 1860 (IPC), could be sufficient to offer legal safeguards for technical interventions.[105] 'Wrongful benefit or harm' is specified in Section 23 of the IPC. In the event of unlawful entry to the 'safe jobs,' this section can be invoked. Section 28, which deals with 'counterfeiting,' will be used to stop people from stealing safe works.

[105]Bently and Sherman, Intellectual Property Law, Oxford University Press, U.K., 200

India is one of the top 20 countries in terms of Internet use. Despite its low Internet penetration rate, India has emerged as the world's software development hub and a popular destination in this sector. With the increased use of the Internet, copyright infringement issues relating to multimedia transmission have worsened. This is a perplexing case. If India offers greater legal safeguards for technical protection policies with few fair use exceptions, the public domain will be depleted, and the public interest concept of copyright will be harmed. If legal security for technical measures is not provided, the Internet can cause havoc with copyright compliance.

The Information Technology Act (IT Act) of 2000 was passed in India to resolve issues posed by 'cyberspace' in the conduct of electronic commerce. The IT Act does not have a clear mechanism for dealing with individual Internet copyright infringement. There are clauses that may be seen as attempting to fix certain facets of copyrights, as shown by Section 43, which deals with penalties for machine and machine abuse.

Non-profit organisations such as NASSCOM (National Association of Software and Service Companies) have been actively participating in the formulation of IT policies and regulations in India as partners with the Government of India and state governments. Its efforts are commendable, as it developed the country's first "anti-piracy" hotline, as well as India's first toll-free anti-piracy hotline. Special police cells are being developed by state governments to combat copyright infringement.

The worries of copyright owners regarding the risks faced by the digital transition are valid. The use of technical defense mechanisms has tipped the scales in favour of right holders at the expense of the public domain. It established a new and effective "Access right" that is used to prohibit unauthorized copying, which is allowed under existing copyright exceptions. Under fair dealing standards, technical safety schemes can be used to avoid infringing replication, reproduction allowed for educational and archival purposes, and reproduction required for science. In India, additional provisions will be added to existing copyright legislation to include legal safeguards for "technological protection initiatives" and "internet rights management." Conciliating private and public interests is difficult; India cannot disregard the public interest principle that underpins copyright laws. It could follow

the lead of Japan, which treats ‘non-commercial' use as fair use.[106]

Fair use should be used as a counterweight to ensure the proper balance between public and private interests in the digital world; there is no optimal approach to the issue of defending copyrighted content in the digital environment. The problem of computer software theft isn't fresh in and of itself. This chapter seeks to discuss problems that exist as a result of providing digital applications on the internet, the way in which piracy happens, the privileges and responsibilities of different parties, and the actions that can be taken to prevent it. The term "computer programmer" is described in section 52(l)(ad) of the Indian copyright Act, 1957, as "a collection of instructions transmitted in terms, codes, schemes, or any other type, including a machine readable medium, capable of causing a computer to perform a specific task or achieving a specific result."

The above is based on the World Intellectual Property Organization's definition; Draft Models Provision for Copyright Legislation. Under the 1977 Model Provisions for the Protection of Computer Software, the concept consists of three parts:

- Computer programmers;
- programmers' descriptions; and
- supplementary information

The speech of the owners of the copyright, not the concept, is protected by copyright law. In India, computer software is shielded by copyright law, which means that only the speech of the software's concept can be covered.[107]

1.8 PIRACY IN DIGITALERA

In India, the film industry is struggling to keep up with rapidly changing emerging and if technology that are challenging current intellectual property laws and market models. Individual consumers can now easily capture, copy, and share films or music in digital form without losing content as technology continues to advance

[106]AnanthPadmanabhan, Intellectual Property Rights: Infringement and Remedies, LexisNexis, Nagpur, 2012.
[107] Harish Chander, Cyber Laws and IT Protection, PHI learning Private Ltd. Publication, New Delhi, 2012, at page no. 14.

globally.[108] Crime in artistic works by collective gangs, which is spawned by such advancements, is a universal concern. Consumers have been pitted against creators of films, music, and television programs, and rights activists are concerned that corporate lobbying is contributing to excessive copyright enforcement that favors producers.

There is agreement on the need for fair copyright rights, but disagreements have arisen about the extent of protection. While these debates continue, file-sharing on the Internet using the peer-to-peer (P2P) paradigm has created a new field of conflict between music and film fans, as well as the respective industries. Using a specific P2P program allows for unrestricted sharing among users.

The challenge of illicit copyrighted content distribution has prompted creators around the world to seek technical solutions. New market models for music distribution have arisen in Western countries with strict copyright laws which are plagued by piracy over broadband Internet. Apple Computer's iTunes pioneered one of these for a la carte music streaming, which was soon joined by related offerings from other major names in the industry. This contrasts with many copyright owners in India's virtual reluctance to accept the advent of digital creativity, which allows for the compression of a vast number of songs for download or sale on compact discs while still integrating tools to protect the content.

While India's piracy issues are true, the entertainment industry has not made a significant attempt to address them with a market-based approach. According to a study conducted by the UK Trade and Industry Department two years ago, piracy cannibalizes 60% of India's film industry revenues. Some states are attempting to combat copyright piracy by enacting tough regulations that allow police to arrest convicted pirates without charge, while the entertainment industry has argued that state governments can assist in re-engaging moviegoers by tax breaks.[109]

Whatever the consequences of these steps, it is apparent that the film and music industry, which is one of the world's biggest, is stuck in a time warp. Unlike in more industrialized countries, the entertainment industry in the country is impacted not so much by P2P providers using the Internet, but by organized gangs using technology

[108]Dr. Gupta & Agarwal, Cyber Laws, Premier Publishing Company, Allahabad, 2010, at pg.no.324.
[109]Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publication, New Delhi, 2012, pg.no.28.

to make large profits by illicit CD replication and selling.[110] The entrainment industry will have to suffer more profit loss as a result of technical improvements in television and radio brought on by digitization, along with broader internet access. The legislation alone could be sufficient to ensure progress in the modern age.

1.9 LET'S SUM UP

We heard in this chapter that the Information and Communication Revolution (ICR), which is currently sweeping the globe, is undermining existing systems and traditions in a way that is difficult to comprehend. Governments are being forced to pass legislation pertaining to the management of information in society due to unprecedented developments in socio-economic organization and democratic governance. The Indian Copyright Act, 1957, is the current intellectual property regime in India that deals with the protection of electronic software. There are no parts of the Act that deal with electronic software theft over the Internet.

1.10 FURTHER READING

- Richard, D, (2004), *Intellectual Property Rights and Global Capitalism: The political Economy of the TRIPs Agreement*, 27 (New York: M.E. Sharpe,2004).
- Hegal,G(2006),ThePhenomenologyofMind(1806),availableathttp://www.marxists.org/reference/archieve/hegal/help/hegelbio.htm (6/08/2006)
- Plant, A (2007) The Economic Theory Concerning Patents for Inventions, 1 *Economica*,30-51
- Anderson B (2003), Rational for Intellectual property rights in the Electronic Age, *New Economy Handbook* (Elsevier Science,2003).
- CarrierMA(2002),*UnravelingthePatent-AntitrustParadox*,150U.Pa.L.Rev.761(Jan2002).
- Roe, S A (1999) Patent 'Monopolyphabia: A Means of Extinguishing the Fountainhead? 49 Case W Res. L.Rev. 509 (1998-1999) at 514; Mark Grdy and Alexander, Patent Law and Rent Dissipation, 78 VA. Rev. 305 (1992) at307;

[110]Tabrez Ahmad, Cyber Law and E-Commerce, APH Publishing Corp., New Delhi, 2003, at Page no.25.

- David M Gould and William C Grubben, (1996) *The Role of Intellectual Property Rights in Economic Growth*,48 J. Dev. Econ. 323 (1996) at333.

1.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Is IPR applicable on Internet. If Yes, then why is not enforceable?**

The cost of reproducing works in digital format is low, and the accuracy of the copies is nearly flawless. Publishers and other copyright holders claim that the Internet harms their intellectual property rights by radically altering the structure and means of publication, leaving their works highly vulnerable to Internet piracy. Because of the Internet's decentralized management, any person can freely disseminate a work on the electronic network known as Cyberspace via any number of networks. A consumer can easily send a job to newsgroups via e-mail or on their personal website.

1.12ACTIVITY

Write a detailed note on need to bring more legislations like the Information Technology Act, 2000 in today's time. (Word count 2000 to 2500)

Unit 2: CHALLENGES TO COPYRIGHTABLE WORK IN CYBERSPACE

2

Unit Structure

2.1 Learning Objectives

2.2 The page and Introduction

2.3 Internet and India

2.4 Why is copyright ill equipped to deal with the internet?

2.5 Basic challenges for Intellectual Property Rights

2.6 Basic Copyright Problems in regards to Internet

- 2.6.1 Determination of Public and Private UseThe-and then she went home and will you be a lack of time that the
- 2.6.2 Problem of Distribution and Reproduction Rights
- 2.6.3 Enforcement of Li on the homepage on, maintaining and they should have the time, and ability
- 2.6.4 Problems which have no solutions

2.7 Copyright in the Age of Napster and Beyond

- 2.7.1 What the evolving napster case stands for
- 2.7.2 MGM v. Grokster
- 2.7.3 Cyber Jurisdiction – the Indian View

2.8 The Future of Copyright

2.9 Let's sum up

2.10 Further reading

2.11 Check your progress: Possible Answers

2.12 Activity

2.1 LEARNING OBJECTIVE

In this chapter, we will learn:

- the meaning of cyberspace and the state of Internet-related issues in India,
- fundamental intellectual property issues,
- why copyright is ill-equipped to deal with the Internet,
- copyright's essential problems in relation to the Internet, including determining public and private usage and enforcing liability,
- The Indian scene in terms of cyberspace control, and
- the future of copyright.

2.2 INTRODUCTION

Cyberspace is a futuristic universe that, while logically only existing in computer memory, is immersive and alive. One can meet and speak to new people in cyberspace, read, write, learn, listen to music, watch videos, look at art, buy and sell items, view government records, submit e-mail, download apps, and get technical help. As more content is uploaded and accessed, and as more people enter the founders of this brave new age, cyberspace is a breathing organism that is continuously evolving. Our legal framework is yet to catch up. This isn't always a negative thing; the legislation always lags behind societal movements before resolving itself. While this modern frontier may never stop emerging, we might also be too early in its development to figure out how to control it. However, as it becomes more embedded (and integral) into our everyday lives, many people are confused with what constitutes appropriate behavior in this modern setting.[111]

The defense of intellectual property — works of the imagination — is one of the most pressing concerns surrounding the Internet. Literary books, images, sound recordings, and other artistic works are protected from being reproduced without the consent of the copyright holder under Sections 13 and 63 of the Indian

[111]Saha, Subhasais&Keshri, Sourav. (2008). Challenges to Copyrightable Work in Cyberspace. 13.

Copyright Act, 1957. It's also uncertain if copyright law would apply to these materials when they surface on the web.[112]

2.3 INTERNET AND INDIA

In India, the Internet infrastructure is rapidly expanding. On August 15, 1995, Videsh Sanchar Nigam Limited (VSNL), a public sector undertaking responsible for all international telecommunication services from India to other countries, launched commercial Internet services. Prior to that, only a few groups had access to the Internet, and the overall number of subscribers was under 10,000. In India, the number of Internet users has surpassed 150,000 and is increasing on a regular basis. People's imaginations have also been captured by the Internet.

According to a survey conducted by the National Association of Software Companies of India (NASSCOM), the demand for Internet connectivity in India is projected to be as seen in Table 1.[113]

While India's Internet users make up a small percentage of Indian the global total, as the Executive Director of NASSCOM put it in a recent post, "if the western world is riding high on the information superhighway, India has begun its effort to be on the Net, by at least building its own information super footpath."

Issues of intellectual property rights (IPR) security are expected to become more prominent as the Internet grows. Currently, the country is focusing on infrastructural growth in order to meet the need for Internet access within a few years.

Table 1 — The demand for Internet connections in India

Year	No. of Connections
1998	4,50,000
1999	8,00,000
2000	1,500,000
2001	3,500,000
2002	8,000,000

[112]Akdeniz, Y., Walker, C. and Wall, D. (2000) The Internet: Law and Society, London: Pearsons Longman p.45

[113] David Bainbridge, Introduction to Computer Law ,Fourth Edition 2000, Pitman Publishing , Edinburgh Gate , England .p 15

The internet has reached every corner of the world. Prioritize the creation of a high-speed national telecommunications backbone and the availability of sufficient telephone lines. To make Internet services more available, nodes have been built in over a dozen cities across the world. The government has agreed to allow private firms to offer Internet services in order to increase access to this advanced and fast means of communication network. With the arrival of private Internet service providers, India could quickly overtake the United States as the world's largest Internet customer, as it did with cable television. The expanded use of the Internet would make IPR security more difficult than it is now. Although the Internet is primed for a quantum leap in the world, it would be premature to propose realistic solutions to the Internet's intellectual property rights concerns, given the lack of experience with such issues. Intellectual property rights (IPR) problems exist now, but they are more theoretical than practical.[114]

The Copyright Act is currently the most powerful tool for dealing with IPR problems on the Internet. The Indian Copyright Act, which was first enacted in 1957, was overhauled in 1994. It has become a forward-looking piece of law as a result of these changes, and the general consensus is that the revised Act is worthy of dealing with copyright problems posed by emerging technology, especially those of the Internet. The Act has adapted to the modern age by dropping some limiting clauses and phrases and extending the meanings of works like cinematograph films (motion pictures) and sound recordings (phonograms) to incorporate certain works in ‘any format' within their purview. It depends, though, on how case laws evolve as Internet IPR disputes are brought to court.

2.4 WHY IS COPYRIGHT ILL EQUIPPED TO DEAL WITH THE INTERNET?

Copyright dates back to the printing press period. Printing presses were operated by a small number of individuals. There was a good benefit as people wanted to steal books, but the pirated books could be traced and were a good indicator of infringement. A typical person could not make a copy of a book and distribute it to friends or sell it on the market. Overall, the device seemed to perform very well. But then came the twentieth century, with its marvelous new inventions. Many of these

[114] David Bainbridge , Intellectual Property (3rd Ed.1996) p 19

advancements, such as photocopiers, tape decks, and VCRs, have altered the relationship between copyright owners and future copier. Although access to computers used to be a deterrent to public copying, modern technologies allowed the ordinary citizen to photocopy papers, tape albums, and archive their favorite television shows.[115] What does one know? The film companies remain as dominant as ever, and copyright is still alive and well.

Copyright is now facing the toughest test ever on the Internet. The first is the simplicity with which it can be replicated. If one wishes to save this file, he would have an exact replica of the original. Furthermore, he could make as many copies as he wanted. The benefit of modern media is that it does not degrade with repeated copies. For others, this is both a blessing and a curse. When faced with a similar situation with the introduction of digital audio tapes (DAT), which allowed for flawless copying of audio recordings, the industry decided to stifle its invention by not allowing second-generation recordings to be made from its tapes (despite intense opposition from the music industry). In addition, the DAT producers charged the record labels a royalty for any tape deck sold, ostensibly to compensate for missed revenue.

Another important factor regarding digital media is the ease of transmission and multiple uses. Another critical aspect of modern media is the speed of dissemination and versatility. For instance, if someone has a copy of this paper on their computer and wishes to give it to one of their mates. He will send it to you via email. Similarly, if he owns a book, he may lend it to him; copyright laws do not prevent this. Once he has the book, he will do whatever he wants about it — this is known as the "first sale" doctrine. He's also allowed to resell it without violating the copyright. While e-mailing this paper to him could seem to be a straightforward analogy to loaning it to him, there is one significant difference: he may give it to him without ever relinquishing custody of it. In other words, he already has a copy on his hard disk, and the other guy now does as well. Where there was once just one, there are now two. This dilemma is exacerbated as you consider the fact that he enjoys the paper and wants everyone to read it. He uploads it to a network rather than sending it to individuals via e-mail. Many people will now read it, copy it, and so on. Who knows

[115]BerntHugenholtz ,Institute for information law ,Faculty of Law ,University of Amsterdam Why the Copyright Directive is Unimportant, and Possibly Invalid.Published in [2000] EIPR 11, p. 501-502 athttp://www.ivir.nl/publications/hugenholtz/opin ion-EIPR.html

how many copies are still out there?

The equivalence of works in print medium is another feature of digital media. Both computer works are nothing more than little bits of data that a computer can interpret. Under the copyright statutes, protectible works of authorship are classified as very particular types of works, with differing regulations and exemptions based on the quality of the piece. Though there are some fuzziness in the distinctions between subjects, it is usually not difficult to differentiate between them. While software programs are called literary works in the case of modern media, the actual effects of such lines of source code may be viewed as a variety of traditional subject matter.

CD-ROM devices, for example, are in the forefront of widely distributed technologies, combining audio and video into immersive games. Virtual Reality is now open to the general population, although in its infancy, and it's only getting better — for both entertainment and science purposes. The World Wide Web, like Gibson's cyberspace prophecy, is a showcase for what these little pieces of knowledge will do on the Internet. Not only could this paper be read by hundreds of thousands of people, but the text is only the beginning.[116]

2.5 BASIC CHALLENGES FOR INTELLECTUAL PROPERTY RIGHTS

The Internet presents IPR administrators with two fundamental challenges: what to manage and how to administer. Only when a consensus on IPR topics in the Internet can be reached can the first challenge be faced. The IPR administrator faces a unique difficulty of balancing the rights of various actors on the Internet, such as content providers, distribution providers, and access providers. This must be accomplished without jeopardizing the free exchange of knowledge while still guaranteeing that the legitimate economic rights of intellectual property creators are not jeopardized. The Internet's intellectual property rights are reliant on it. If the IPRs on the Internet have been determined, the task for the IPR administrator is to determine the most cost-effective way to implement them.

[116] Niels Ferguson ,Censorship in action:why I don't publish my HDCP results August 15, 2001at http://www.macfergus.com/niels/dmca/cia.html

Although there are no two minds on the importance of securing IPR on the Internet in the interests of authors, the implementation of such rights over this medium is likely to be difficult due to the technical device's sophistication. The compliance mechanisms would almost certainly necessitate the use of costly and sophisticated electronic equipment. After all, "the machine's response is the machine," and each new machine appears to be more expensive than the previous one. Will the costs of the interventions become so high that developed nations are forced to abandon the Internet? Would the protection of intellectual property rights on the Internet result in the planet being divided between those who have access to technology and those who do not? When it comes to the IPR problems of the Internet, these are the sorts of issues that must be answered.

In India, the Internet is still in its infancy. The majority of the questions posed in this paper are hypothetical and have not been encountered in reality. However, in order to accelerate the development of the Information Superhighway without jeopardizing the rights of copyright owners, it is important to investigate them thoroughly and find solutions. The golden mean between the general interest and the interests of the authors and disseminators of copyright works should be sought.[117] Around the same time, the latest IPR standards would not result in a widening of the gap between developed and emerging countries.

2.6 BASIC COPYRIGHT PROBLEMS IN REGARD TO INTERNET

2.6.1 Determination of Public and Private Use:

Determining the line between private and public use is one of the most fundamental copyright problems on the Internet. The Indian Copyright Act, like all copyright laws around the world, distinguishes between copying for public and private use. Reproduction for public use requires the consent of the right owners, while the statute permits equal dealing for private use, study, critique, or analysis.[118] This distinction is undermined by an individual's freedom to distribute some copyrightable

[117] John Naughton ,A conspiracy against the public Online commentary Sunday March 16, 2003 at http://media.guardian.co.uk/newmedia/comment/ 0,7496,915043,00.html

[118] Charles Clark, General Counsel, International Publishers Copyright Council Copyright Representative, Federation of European Publishers, The copyright environment for the publisher in the digital world http://users.ox.ac.uk/~icsuinfo/clark.htm

work to a large number of users simultaneously over the Internet from the privacy of his or her house, and users' ability to receive a perfect copy of the material distributed simultaneously in their homes. Many believe that the disappearance of the fine line between public and private lands necessitates a new generation of copyright norms.

Any common ideas have been turned on their heads as a result of the Internet. The publishing industry is a good example. Publishers of books and music had entered the market with the start of the industrial revolution and the era of mass manufacturing. They've been so ubiquitous that authors can't imagine a future without them. The Internet, unlike books, is a tool that eliminates the intermediary between a writer and his or her reader. The author may publish his or her work on the Internet, which the reader can see directly. If the printing press gave birth to the publishing industry, the Internet has sounded an alarm bell, if not the death knell, for that industry by encouraging every writer to be his or her own publisher. This begs the issue of whether or not making a work available on the Internet qualifies as "publication." For the purposes of copyright, the Indian Act defines ‘publication' as ‘making a work accessible to the public by issuing copies or communicating the work to the public.' Because of its non-restrictive nature, this term can be interpreted as including electronic publishing and, as a result, ‘publication' on the Internet. However, it will take a few years for electronic publication to make a significant impact in India.

The question of whether communicating over the Internet qualifies as "public contact" remains unresolved. The Indian Copyright Act has a detailed description of "public correspondence." According to the Act, "communication to the public" requires "making any work accessible for the public to view, hear, or otherwise appreciate directly or by any means of exhibition or diffusion other than issuing copies of that work, regardless of whether any member of the public currently sees, listens, or otherwise enjoys the work so made available." This term is considered broad enough to include Internet networking within its scope. If the courts take this opinion, Internet service providers in India would have a difficult time determining who owns the rights to the Internet's content.

2.6.2 Problem of Distribution and Reproduction Rights:

The distributing right in Indian law, like most copyright laws, is exhausted with the first transaction. Currently, a student may freely sell a used textbook, and a library may freely distribute the books it has bought among its representatives. Since no copy can be transmitted without replication on the Internet, dissemination becomes entangled with reproduction.

On the Internet, the freedom to reproduce raises a number of serious issues. This is due to the fundamental essence of Internet transmission. Any stage of transmission involves reproduction. Temporary copying (also known as caching)[119] is an essential aspect of the Internet communication mechanism through which messages will not be able to pass across the networks to reach their intended destinations. And if a user just needs to browse, transient copying occurs on the user's screen. Coverage of temporary reproductions was a contentious topic at the December 1996 World Intellectual Property Organization (WIPO) Diplomatic Conference, which ended in a deadlock. Can a reproduction be prohibited where it occurs in the form of permitted use of the work and its primary objective is to make the work visible, or when the reproduction is of a temporary or incidental nature? Reproduction in India is required to be in a physical way, but it also requires "storing it in any medium through electronic means." Case rules are yet to specify whether reproductions occurring in Internet correspondence are covered by the law's right of reproduction, but views on temporary and permanent reproduction, as well as the validity of temporary reproduction, will continue to differ.[120] It would be curious to see how the courts add the idea of economic relevance to a reproduction in order to get it under the Copyright Act's right to reproduction.

2.6.3 Enforcement of Liability:

The problem of responsibility is perhaps the most important one in terms of copyright law. For one thing, there's the question of responsibility for actions committed during

[119] Justice Laddio, "Copyright, Over-strength, Overregulated, Over-rated", (1996)5 EIPR 253.
[120]Prof.J.E.Cohen (1998) , Some Reflections on Copyright Management Systems and Laws Designed to Protect Them, 12 Berkeley Tech L.J. 161 at 169

the delivery of a legitimate (as opposed to an infringed) copy of a work. As previously mentioned, the question is highly dependent on the judiciary's view of different legal rights. If the courts decide that in-transit copying, for example, is a breach of a patent, so concerns about damages will emerge. Who should be made accountable? Who sends the job out, who gets it, and who is the Internet service provider (ISP)? The solution may not be simple to come by. The other thing is the transmission of a specifically infringed copy of a job over the Internet. The question here is whether an ISP should be found responsible for a subscriber's copyright violation even though he is unaware of the subscriber's behavior.

According to Section 79 of the Information Technology Act of 2000, where the subscriber may show that the crime or contravention was done without his knowledge or that he used any reasonable efforts to avoid the offence or contravention, he would not be found responsible under the Act. The Indian Copyright Act stipulates that the violation or abetment of the infringement must be done "knowingly" by an individual while defining copyright offenses. It is likely that, because of the word "knowingly," an ISP, which might or might not be aware of the subscriber's copyright violation, may be exempt from prosecution and penalty. This, though, poses a new problem. Even if the ISP is not criminally liable under Indian law, he can be held liable under the laws of another region. How will we control this, given that the Internet is completely universal and does not respect national borders? The networks are scattered around the globe, and a message or piece of information may pass through many countries before arriving at its final destination. The ISP may not be liable in the country of origin or the country of destination, but it may be liable in a transit country. Second responsibility arguments of contributory or vicarious violation make ISPs and software developers legally responsible for copyright infringement. A contributory infringer is described as "one who, knowing of the infringing behavior, induces, triggers, or materially contributes to another's infringing actions." In order for the provider to be found liable, there must have been an actual violation, and the provider must have committed some contributory or vicarious copyright infringement.[121]

[121]ThiliniKahandawaarachchi, Liability of ISP for third party online copyrights infringement: A study of the US and Indian Laws, journal of intellectual property rights,Vol 12, pp 553- 561, Nov 2009

The regulation of national IPR rules, which are bound by federal jurisdictions, raises difficult challenges in the seamless world of the Internet. This is an environment where international harmonization of laws is critical; otherwise, the possibility of litigation in some countries which force the Internet service provider to examine the content being distributed for copyright approval, causing the whole procedure to be delayed. This could turn the Internet into a "World Wide Wait." The aim should not be to stifle knowledge flow, but rather to accelerate it.[122] A paradigm change occurs with any significant technical advancement, and the Internet is no different. New norms will be required to assign liability to the appropriate parties; an Internet service provider is not always an enabler of copyright infringement.

The variety of challenges that the Internet presents for IPR protection makes us wonder if copyright legislation would be adequate to face the burden, or whether we should pursue a unique IPR protection scheme. In reality, to face the current technical demands, there is a widespread movement to think in terms of unique ways of defense. Designer rules for intellectual rights of manufacturing designs, plant types, and integrated circuits have thus been enacted. Sui generis security is being considered for databases and folklore. Although copyright laws have become more flexible over time to accommodate modern ways of production, they do have a lot of rigidity.[123] Copyright does not cover inventions, processes, or technical features because of the idea-expression dichotomy, which is fundamental to the copyright doctrine. A sui generis type would, by definition, have much more versatility in terms of its reach, level, and duration of security. But it also requires a desire to try new things, as well as a willingness to let the legislation change by trial and error.

2.6.4 Problems which have no Solutions:

Differences in cultural perspective can have an effect on the appropriateness of content communicated over the Internet in some cases. Many literary, musical, and cinematic expressions that are permissible in western cultures may not be

[122] Raman Mittal, online copyright infringement liability of internet service providers, journal of the indian law institute [vol. 46 : 2]

[123] R. MurugaPerumal, Copyright Infringements in Cyberspace: The Need to Nurture International Legal Principles, International Journal of The Computer, the Internet and Management Vol. 14.No.3 (September-December, 2006) pp 8-31

acceptable in more conservative societies such as India. A national government may exert some restrictions on books, music, literary works, and cinematographic films; this is also possible to a large degree for broadcasts and telecasts. How can we do this in the case of Internet communication? It is impossible to provide police at national borders on the Internet. Controlling and filtering content that spreads across the Internet presents a number of functional challenges. It is possible to intercept content that is indecent in nature (prurient or lascivious) under Section 69 of the IT Act, which currently provides the ability to ban websites. Such action may also be taken against pornographic websites, which is why there isn't any pornography hosted in India. And so, the Internet is also much too big and amorphous to be controlled.[124] When an infringing site is blocked, a hundred more can appear in different locations. The amount of knowledge available on the Internet is enormous, and it is spread out across the world, not just in one region. Any government will be unable to censor it. When media sources are small, censorship is a possibility. There is a significant distinction between traditional broadcast channels such as television and radio and the Internet. There is one broadcaster and many viewers or listeners in the former, while an overwhelming number of ‘netizens' are concurrently inputting and viewing information in the latter. What kind of technological devices are capable of regulating the Internet's dynamic matrix, in which any consumer point is also a production point?

2.7 COPYRIGHT IN THE AGE OF NAPSTER AND BEYOND

2.7.1 What the Evolving Napster Case Stands for:

The Napster case, including Judge Patel's well-researched decision granting the record label and music distributor plaintiffs a preliminary injunction, and the 9th Circuit's further review of the fair use factors posed as an affirmative defense by Napster,[125] illustrate the extraordinary way the patchwork copyright legislation responds to the current complexities of the Internet. Although Napster may be extending the metaphor to make it sound rational and reasonable, the definition and

[124]Aakanksha Kumar, Internet Intermediary (ISP) Liability for Contributory Copyright Infringement in USA and India: Lack of Uniformity as a Trade Barrier, Journal of Intellectual Property Rights Vol 19, July 2014, pp 272-281

[125] https://core.ac.uk/download/pdf/205213553.pdf

enforcement of "compulsory" music licensing is one of the most complicated (and misunderstood) facets of copyright law, and should not, in the authors' view, be loosely applied to other aspects of the music marketplace. It's also worth noting that compulsory licensing rules are incredibly strict, requiring, among other items, advance warning before sale. Failure to provide adequate notice effectively eliminates the chance of a compulsory license and makes producing and distributing illegal. And now, Napster is pressing Congress to enforce a sort of "compulsory" license on record labels for digital downloading, similar to the compulsory licensing clauses of the copyright legislation that exist to prohibit monopolies of mechanical licensing of musical works, of digital downloads of sound recordings.

Against this backdrop, in January 2002, for the first time since Napster was shut down in the summer of 2001 under Judge Patel's preliminary injunction order, as affirmed by the 9th Circuit, Napster has introduced a demonstration of a commercial file-swapping technology, using tracks licensed from independent record labels. Judge Patel's Napster decision followed a conventional approach to copyright law and preliminary injunctions, and it was arguably distinct from most copyright and technology cases. The plaintiffs copyrighted the bulk of the songs and records made available for free downloading on Napster, and it was apparent that Napster never requested or received licenses. In internal records and on the record, the Court consistently emphasized Napster's expertise, purpose, willfulness, and lack of honesty, as well as the "vast scope" of the violation affecting "millions" of consumers and the "usurping" impact on record companies' online music markets.

'The majority of VCR purchasers in Sony did not distribute recorded television programs, but merely enjoyed them at home,' the Court noted in separating Napster from the Sony case. A Napster user who downloads a copy of a song to his hard drive, on the other hand, can make the song available to millions of other people, even though he later decides to buy the CD. So-called sampling on Napster can exponentially encourage illegal distribution,' and that "Napster users may retain the music they download." In ruling that Napster use does not represent "family or home use in the usual context," the Court also pointed to the "global size" of Napster use. Napster's reasons for extending "time-shifting" to "space-shifting" and adding "the Ninth Circuit's claim, in a case concerning an inapplicable law, that space-shifting

constitutes non-commercial personal use" were all dismissed by the Court.

2.7.2 MGMvGrokster[126]:

In this case, the Court opted to apply the standard test for contributory infringement and vicarious liability rather than the Sony rule. In this situation, the technology is s and omewhat different from Sony's. The Court holds that a product seller will be held responsible for copyright infringement by a third party if they "distribute a gadget with the object of encouraging its use to infringe copyright, as shown by plain speech or other affirmative measures taken to promote infringement, going beyond mere delivery with knowledge of third-party action," as shown by "clear expression or other affirmative steps taken to foster infringement, going beyond mere distribution with knowledge of third-party action." According to the Court, it would be "impossible to enforce rights in the covered job efficiently against all direct infringers," so the only practical solution is to pursue secondary responsibility against the device's distributor. Since there was "no proof that Sony had desired to bring about taping in breach of copyright or taken aggressive action to maximize its revenues from illegal taping," the Court differs from its previous decision in Sony. When deciding whether or not the individual was facilitating infringement, the Court looks at motive. Grokster sought to encourage copyright infringement by soliciting business from former Napster users, not attempting to restrict infringement by consumers using their apps, and profiting financially from the selling of advertising, according to the evidence.

2.7.3 Cyber Jurisdiction — the Indian View:

Until 1999, India's cyber authority was almost non-existent. For starters, interstate conflicts never reach the threshold of private international law in India as a result of the country's highly unitary government model. As a result, India has seen little production of private foreign positions. Furthermore, there have been few cases in Indian courts requiring Indian courts to have authority over a foreign matter However, when the Internet and e–commerce shrink boundaries and merge regional and tribal limits on authority, such a jurisprudential growth will become critical in the near future. There are two situations that need to be considered:

[126]545 U.S. 913

(a) The manner in which international courts assume control over Internet-related matters, and
(b) The implications of a foreign court's decree.

The laws to remember when using electronic data interchange (EDI), e-commerce, electronic fund transfers, electronic currency, copyright, intellectual property rights, digital signatures, and so on.[127] While the Information Technology Act has protections for digital signatures, the Evidence Act also needs to be amended to recognise them. To accept new innovations, changes are also expected in the Indian Penal Code, 1860, the Evidence Act, 1872, and the Indian Patents Act. Any court with exclusive authority over the matter is granted jurisdiction under Section 62 of the Indian Copyright Act, 1957. It also moves on to clarify the courts' jurisdictional boundaries. The Information Technology Act, once again, allows for extraterritorial control in cases of cybercrime. Section 74 of the Indian Penal Code states that any offense involving a machine or computer resource in India can be prosecuted under Indian law.

2.8 THE FUTURE OF COPYRIGHT

Since the existence of the Internet is still too unclear, there is no correct response to the issue of copyright's security. Obviously, the decisions we make today will have an impact on the path it will go. Copyright isn't intended to give its owners complete ownership of their works; rather, it's a very specific set of rights intended to encourage innovation in the public interest.[128] A more appealing option would be to view fair use widely to prevent misuse by noncommercial, nonharmful uses. Whatever the outcome of copyright disputes, it is clear that other forms of creator compensation will coexist on the Internet. VSNL, for example, offers "live" performances in which celebrities enter chat rooms and engage with customers. Professional assistance is provided by software providers. On the Internet, there are a plethora of free intellectual works available, all of which clearly state the terms by

[127]Priyambada Mishra and Angshuman Dutta, Striking a Balance between Liability of Internet Service Providers and Protection of Copyright over the Internet: A Need of the Hour, Journal of Intellectual Property Rights Vol 14, July 2009, pp 321-329
[128]FarnazSaadat, Mohammed soltanifar, The role of ISP in encouraging customers to use their internet services in Iran, International journal of business and social science, Vol 5 no 3 march 2014.

which they can be reproduced or used. This article, for example, can be written in any format as long as it is correctly attributed and not distributed for profit. New forms of compensation can eventually dethrone copyright. Maybe, in the end, public views of copyright on the Internet would be more important than stringent legislation. Laws, it is said, are intended to represent rather than regulate public sentiment. People adhere to laws that they consider to be fair. 'A societal over-reliance on barricades rather than conscience would inevitably wither the latter by making burglary and stealing into a competition, rather than a crime,' wrote John Perry Barlow in reference to cryptography. The future of copyright in cyberspace can be better determined by people's common concepts of what is equal and equal.

2.9 LET'S SUM UP

We learned in this chapter that copyright has a direct relationship with cyberspace. Copyright security on the Internet is fraught with issues. These issues and concerns must be addressed with caution and patience, taking into account the current situation in the post-Napster period and beyond.

2.10 FURTHER READING

- Barlow J P, The economy of ideas
- *A & M Records* v *General Audio Video Cassettes Inc*, 948 F Supp 1449, 1456 (C D Cal1996).
- James T C, The Internet as a challenge for intellectual property protection: An Indian perspective, *World Intellectual Property Organization Seminar for Asia and the Pacific Region on the Internet and the Protection of Intellectual Property Rights*

2.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What does "Communication to the Public" means and where is it defined?**

Home and Communication over the Internet is considered "public communication," and it is still a controversial subject. The Indian Copyright Act has a detailed description of "public correspondence." According to the Act, "communication to the public" requires "making any work accessible for the public to view, hear, or otherwise appreciate directly or by any means of exhibition or diffusion other than issuing copies of that work, regardless of whether any member of the public currently sees, listens, or otherwise enjoys the work so made available."

2.12 ACTIVITY

Write a detailed note on how copyright has a direct relation to the sphere of cyber space. (Word count 2000 to 2500)

Unit 3: PRIVATE INTERNATIONAL LAW AND INTELLECTUAL PROPERTY RIGHTS ON THE INTERNET

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Bilateral rules

3.4 Neutrality of Contract

3.5 Contract on the Internet

3.6 Contractual relationships

3.7 Copyright on off-shore locations

3.8 Meritless intellectual property right holders

3.9 Extra-contractual liability

3.10 IPR, Internet and legal system

3.11 Let's sum up

3.12 Further reading

3.13 Check your progress: Possible Answers

3.14 Activity

3.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- The relationship between IPR, Internet, and its related aspects in cyber governance.
- International treaties and conventions with respect to Private international law
- Various provisions of treaties and conventions governing the Internet laws.

3.2 INTRODUCTION

The Tools of Private International Law

1) Points of Contact with Any Kind of Contract or Right The status doctrine was the beginning of private international law. When traders began to migrate to international markets, the issue of their legal status emerged. Many problems were regulated by one's personal status. Friedrich Karl von Savigny later introduced a scheme of contacts, according to which the law of a given country that is the center of gravity of the is regulated by the law of the State whose policies will be most legitimate relationship is deemed applicable for eac and h significant type of rights or contracts. Only the United States continues to fail to use this tool. Finally, national or regional codification of private international law tends to be the final move, with more than 60 Acts regulating conflicts of law in countries outside Europe and at least 17 Codes on conflicts.[129]

The fusion of Savigny's approach and the codification movement yields a detailed plan for intellectual property protection on the internet, which will be discussed at the conclusion of this post. These ideas are a practical implementation of the concept of the closest possible connection between a given right or contract and national legislation. The closest relation is not to a state, but to a series of laws that can be traced back to a specific legislature.[130]

The nearest link triggers a series of checks. The first and most important measure refers to the legal rules controlling the characteristic results, the second to the legal rules that apply when any harm is currently felt, and the third to the collection of legal

[129]EDWARD I SYKES & MICHAEL C PRYLES, AUSTRALIAN PRIVATE INTERNATIONAL LAW 1 (3rd ed. 1991).
[130]PB Carter (1990) 6 BYIL 400, 402.

rules that typically apply to the respondent's activities. As can be seen below, those laws have a simple subsidiarity, but they are all subject to different exceptions.

2) Points of Contact Exceptions by Category The governing principle of the nearest link, as well as other significant laws, result in at least three exceptions:

a) Where the facts of the case prove that the matter is reasonably beyond the scope of another legislature, courts may apply a law other than the one deemed valid by the particular clause.

b) A third country's direct implementation laws can be used where public or private interests warrant it. Antitrust laws and other long-arm regulations, for example, can take precedence over the rules that would otherwise apply.[131]

c) There are two types of renvoi: remission and propagation. When the lexfori designates the rule of another state as the relevant law, but the designated law deems the lexfori to be applicable, there is a remission. When the lexfori declares another law to be applicable and that law declares the law of a third State to be applicable, there is a transfer. While the Rome Conventions I and (draft) II prohibit renvoi, we believe that where certain texts or related ones are not valid, remission or dissemination can be used intelligently in situations concerning the right to advertising, libel, and droit moral obligatoire resulting from the Internet.

Consider the example of a well-known actress's name (Isabelle Adjani) being misappropriated as a domain name. If the argument were to be heard in Switzerland, the French actress would be able to chose between the law of her place of residence (Switzerland) if the wrongdoer should have foreseen that the injury would occur there, and the law of the wrongdoer's ordinary place of residence or place of business if the wrongdoer could have foreseen that the injury would occur there. There would be remission if the wrongdoer's country's private foreign law had referred the case to Swiss law. There would have been transmission if the matter had been transferred to the statute of the wounded actress's nationality (in our case, French law). There would be no renvoi if the court decided that both the affected party's law and the wrongdoer's law pointed to the same practical remedy, as the WIPO Panel did in the case of Mrs. Adjani, so there would be no clash of laws.

---

[131] Book length studies include: JAMES J FAWCETT & PAUL TORREMANS, INTELLECTUAL PROPERTY AND PRIVATE INTERNATIONAL LAW (1998);C WADLOW, ENFORCEMENT OF INTELLECTUAL PROPERTY IN EUROPEAN
AND INTERNATIONAL LAW (1998).

If the forum is a country where internet litigation is rare, the renvoi could result in a law that is more developed on internet issues than the lexfori. If, on the other hand, the forum's case law is already well-developed, as it happens to be in the United States, remission provides a clear means to apply the case to well-established requirements rather than a blank international law. Any approach that favors the enforcement of an established body of law is conducive to global judicial harmonization in and of itself.

3.3 BILATERAL RULES

A general observation on the procedures of contemporary private international law should highlight the bilateralism of dispute resolution rules: regardless of whether country A or country B is the forum's country, the same test is used to decide whether the law of country A or country B is relevant. The forum's legislation is not favored by bilateralism.

3.4 NEUTRALITY OF CONTACTS

The rules of conflicts must remain neutral. They should not systematically lead to the law affording a higher level of protection for intellectual property rights. However, in the long run, the current scheme, which is based on the rule of characteristic efficiency, may lead to a widespread implementation of developing country rules, since they are the primary producers of protected intangibles, at least as long as traditional medicine and folklore are not highly protected.[132] This may or may not be interpreted as implying that a high degree of intellectual property rights boosts a region's innovation. Is the higher expenditure cost, though, due to the regulatory system governing intellectual property rights, or is it due to other factors? The internet may help developing countries assert their own creativity on the internet, or, as has been seen with the movie industry, globalization may lead to concentration of power. Macro-economics provide no clear answer. It is therefore important that the rules on conflicts of law remain neutral.

[132] DAVID GODDARD, CONFLICT OF LAWS: JURISDICTION AND FOREIGN JUDGMENTS 4 (1999).

3.5 CONTACT ON THE INTERNET

Let us take an example. A producer established in country A commissions a poster from an artist who resides in country B. Since this poster is part of a larger promotional campaign of 200 other posters, he retains the freedom to change it to suit the others. However, a computer programmer in country C steals the completed poster from the artist's computer and posts it on his webpage, which is hosted by a server in country D, in a revamped format. From there, the poster is downloaded for a fee in 100 countries (E1 to E100). The criminal law of countries B and C applies to the electronic theft, but private international law will govern the conflicts concerning the artist's droit moral, the interpretation of the commissioning contract, and the producer's rights vis-à-vis third parties who have downloaded the poster. This example illustrates how a simple international case can require examination of three types of relationships:[133]

1) contractual;
2) extra-contractual (arising out of the infringement of intellectual property rights); and
3) quasi-contractual (for the accounting of profits, if any).

There is no doubt that contractual relationships are the key element in the application of technical measures to safeguard copyrighted contents on the internet. The seamless coordination of business operations on the internet is enabled by a network of interconnected contractual arrangements, allowing other companies or users to completely profit from the e-facilities. Liability for tortious conduct and the ensuing accounting for profits are nonetheless necessary. These three aspects shall now be considered from conflicts of law perspective.

3.6 CONTRACTUAL RELATIONSHIPS

1) General Rule

The legislation applicable to a deal entered into on the internet or for the use of an intellectual property right on the internet, according to Article 4, paragraph 2 of the

[133] See further Graeme W Austin, *Social Policy Choices And Choice Of Law For Copyright In Cyberspace*, __Oregon Law Rev. __(2001) (forthcoming).

Rome Convention of 1980, is the law of the country where the supplier of the characteristic performance has his domicile or establishment. This rule applies to all licensing or transfer of intellectual property rights. The practice tends to mention "transfer of rights" where the word "licensing" would be more technically correct.[134]
Therefore, in determining the applicable law, no distinction should be made between an outright transfer and a sheer license. Furthermore, the so-called "license" allowing the use of software or any intangible embodied in a CDRom or other physical copy is often ancillary to the selling of the copy and, as such, should be subject to the same laws as the sale.
In the absence of a separate option of law by the parties, both the selling and the license of intangibles will be subject to the licensor's or seller's regulation. Consumer rights legislation has been set aside. There are still several other drawbacks to consider.

2) Transnational Law

There is no conflict of laws where the laws potentially applied in a particular situation do not differ on the points in question. This is most often the case where a higher authority has mandated some level of harmonization, as is the case in Europe. Non-interference of State law with practice, on the other hand, will result in harmonization.

- Licence Law

This second situation arises on the internet in the absence of applicable State law. Furthermore, as merchants usually resort to arbitration rather than to State courts, it is possible for a transnational law to emerge. The basis of this law is hotly disputed between supporters of the lexmercatoria and sovereignists. Whatever the merits of the lexmercatoria, licensing practices are identical worldwide and most municipal laws are silent on details. Thus, the ideal conditions are met for a transnational body of law to come into existence. Here are two examples:

1) Although still uncertain two decades ago, the right of an exclusive licensee to sue for infringement is now recognized in most jurisdictions. Canada also

[134] See generally, J FAWCETT (ed.), DECLINGING JURISDICTION IN PRIVATE INTERNATIONAL LAW: REPORTS TO THE XVITH CONGRESS OF THE INTERNATIONAL ACADEMY OF COMPARATIVE LAW: ATHENS, AUGUST 1994, (1995).

permits the holder of a non-exclusive license to sue the infringer, but this continues to be a pioneering step that has yet to catch on.

2) The truly exclusive licensee's privileged status is linked to his duty to use the product, patent, concept, model, or patented art. As a result, the licensor who promises not to use the technology will almost certainly be compensated. However, in the case of "sole licensees" (who must consider competition from the licensor but no other licensee) or "semi-exclusive licensees," transnational legislation is less simple (who enjoy the status of an exclusive licensee in some countries or for some applications of intellectual property rights, and the status of a sole licensee in other areas). French, German, and Swiss law, in our opinion, have all agreed on the universally recognized doctrine for genuinely exclusive licensees. However, while French law acknowledges the need to use intellectual property rights even for non-exclusive licenses, this remedy cannot be considered part of the transnational licensing law. On the internet, no conflict of law exists because alternatives are transnational.

- Competition Law

The internet is also subject to similar or identical solutions in the field of competition law. When the time came to develop a world-wide system for the assignment of domain names, a common understanding between the U.S. and European authorities on antitrust issues helped persuade the U.S. to surrender its monopoly in this regard (as well as the initiation of proceedings by the E.U. competition authorities, which were later summarily dismissed). The next reform of the European block exemption regulations can also take into account the current state of antitrust and licensing law in the United States.[135]

- Consumer Protection

In the United States, Professor Raymond Nimmer's efforts to compile the licensing law in Article 2B of the Uniform Commercial Code finally led to a Model Act to

[135] Andrew F. Christie, 'Private International Law Issues in Online Intellectual Property Infringement Disputes with Cross-Border Elements: An Analysis of National Approaches' (World Intellectual Property Organization, 2015)

Protect Consumers (Uniform Computer Information Transactions Act, hereafter UCITA). Its adoption is pending before several State legislatures. As the sole restatement of modern licensing law, the UCITA will be an inspirational model in many countries.

The UCITA regulations on conflicts of law are symptomatic in that they defend customers, but with a caveat: the parties should select the relevant law. However, their choice will not be enforced in consumer contracts if it modifies mandatory provisions of the applicable law under the UCITA. To a certain extent, European laws also purport to help consumers by having the mandatory provisions of their own laws apply. It's odd because the consumer's home country's law is assumed to be more favorable than the seller's home country's law – which, logically, cannot be valid in both situations when sellers and vendors are more or less involved in the same developing countries. Nonetheless, the rationale for applying the consumer's law is to help avoid any surprise to him or her. As a result, it is preferable to allow the consumer's country's law to prevail in order to promote the advancement of e-commerce, especially in those European countries where there is a reluctance to engage in large-scale e-commerce.[136]

The legal condition is similar to ordinary distance trading where an order is made on the internet but the items are shipped later by courier or postal. When downloading intangibles, however, it is important to differentiate between material that is not covered by intellectual property rights and content that is. The buyer can be shielded by his or her own statute where no intellectual property rights are involved. Where copyright, architecture or model legislation, or a sui generis privilege on data extraction applies, the licensor's law should apply rather than the consumer's law, since the clauses of the law relating to licensing deals are a lexspecialis in terms of consumer protection laws, which are best suited to licensing transactions. The text of Article 5 (1) of the Rome Convention may also be used to make a more formal argument: permits are not arrangements for the supply of goods or services.

Finally, licensing necessitates a balancing act since the greater a country's legal security is, the more relevant it becomes to still extend the exceptions offered by that country's rule. For example, Anglo-American copyright law provides a low threshold for originality but has a broad exemption from protection for what is known as "fair

[136] Graeme B. Dinwoodie, 'Developing a Private International Intellectual Property Law: The Demise of Territoriality?' (2009). Oxford Legal Studies Research Paper No. 52/2009.

use" in the United States or "fair dealing" in the United Kingdom. If the licensor is located in the United States, a European user forum can apply the fair use exception even if his or her national legislation does not permit it, and even if the fair use exclusion is more of a substantive copyright law provision than a contract law provision.

- Exceptional Application of the Licensee's Law

But for consumer rights or antitrust law purposes, the proposition mentioned above applies to the licensor's law being relevant. It is important to remember that other extraordinary situations can necessitate the implementation of the licensee's country's rule. In this respect, three examples are worth noting.

3.7 COPYRIGHT IN OFF-SHORE LOCATIONS

When a supplier of intangibles on the internet is an efirm with no particular relationship to the jurisdiction of any State, the general provision for diverging connections or the inspection of the nearest communication could contribute to the implementation of the licensee's statute. Any businesses in Panama or the Netherlands Antilles, for example, may be considered to be in this group. It is suspected that such companies would unlawfully misuse the intellectual property of serious right holders and distribute it around the internet. Their motivation may be direct remuneration from internet users, payments from advertisement sales, or income provided from the sheer accumulation of checked e-mail addresses.[137] In and such a case, the courts will break from the fundamental tenet that the relevant statute is determined by the licensor's characteristic results. In the 160 member states of the Paris Union, the 147 member states of the Berne Union, and the 134 countries that have signed the TRIPS Agreement, intellectual property theft is prohibited. It is fair to conclude that a deal allowing for the sale of such pirated intangibles would be declared null and invalid in these countries, and contra bonos mores in the remaining countries. As a result, an illegal or unethical duty cannot be a characteristic obligation under the Rome Convention.

[137] ICT Development Index (2017)

If the implementation of the nearest relation test may not be accepted for this first explanation, a second reason could seem to be more in line with legal and economic thought.

3.8 MERITLESS INTELLECTUAL PROPERTY RIGHT HOLDERS

If the licensor does not obtain the intellectual property right through its own purchases, actions, or ingenuity, or at a fair price, or through inheritance or acquisition, the licensor has achieved nothing characteristic until the licensing agreement is established. Intellectual property regulations aim to safeguard intellectual assets. Piracy is not regarded as an expenditure worthy of security. Furthermore, an e-business that thrives on the illicit manipulation of others' intangibles is unlikely to have funds that could be seized to pay its creditors in the event of a default. The underlying reason for the theory of characteristic performance is the connection between the country of the principal place of operation and the country in which bankruptcy proceedings or disciplinary actions will be instituted if the debtor of the characteristic performance may not discharge himself or herself of his or her obligations.

The foundation of the structure is the consistency of the law governing contract efficiency and the law governing compliance procedures. When the efirm, on the other hand, has no tangible properties, the off-shore climate would be ignored in favour of the licensee's legal environment.

3.9 EXTRA-CONTRACTUAL LIABILITY

1) Scope of the Extra-Contractual Liability

Intellectual property rights abuses occur often where there is no valid contractual arrangement between the parties. It's possible where the parties claim to have signed a deal, but the contract isn't binding unless a form condition isn't fulfilled, for example. Then, under Article 8 of the Rome Convention, the rule that would have

held if the contract had been legitimate is declared applicable. However, we will only discuss violating acts and unfair competition in the following sections.[138]

In the one side, there is a difference to be made between patent law and copyright, trade name, and trademark law. Since patent law is so closely tied to national economic policy, it is far more territorial. As a result, a list of contacts with each of the major intellectual property groups would be proposed. However, writers have previously gone into more detail on copyright and legal disputes. As a result, we'll begin our investigation with copyright and neighboring rights.

2) Copyright and Neighboring Rights

a) Characterization of the country of "origin"

The definition of "country of birth" is central to the Berne Convention. This point of touch is responsible for determining whether a job is covered in other Member States (alternatively the nationality of the author). It also aids in the distinction between "domestic" and "international" works, which are works of the same origin as the forum and do not benefit from the Berne minimum requirements of security.

Finally, it is important for the reciprocity provision that remains in the Convention, such as the period of defense and works of applied arts (but not for a "droit de suite"). The "country of origin," in our opinion, is a convention-specific term that cannot be twisted into a new and distinct concept for the Berne Convention's purposes. When it comes to conflicts of law, on the other hand, the criteria may be voluntarily selected or construed by States because the The ordinary residence or domicile of a citizen is a more important touch than his or her nationality, according to modern codifications of private international law. It's just reasonable that the author's address is the primary point of touch regarding copyright issues, as well as perhaps deciding whether or not there is a protectible subject matter.

b) Place of acting

Infringement of intellectual property rights faces the same challenges in establishing a conflict of law contact as more conventional tortious behaviors. When the breach and the resultant destruction happen on the same piece of land, the rule of that state will apply. In the internet, though, it is more likely that the breach will occur in one place but the harm will occur elsewhere. As a result, some scholars designate the State in which the most recent infringement occurred as their primary touch. This

[138] Lilian Edwards, 'The Role of Internet Intermediaries in Advancing Public Policy Objectives Forging Partnerships for Advancing Policy Objectives for the Internet Economy, Part II' (OECD, 2011)

confrontation law is widely agreed for tortious actions to some degree. Most European regulation, on the other hand, leaves the option of the rule of the state where the harm occurs free. In this case, the Swiss private international law codification is a stronger model. Article 110 (2) of the Swiss Federal Law on Private International Law ("PIL") retains the concept of territoriality in the context of intellectual property, with the caveat that the parties can opt for the lexfori ex post facto.

However, we have found that the territoriality principle is not useless on the internet. As a result, we can turn to the plethora of rules governing personality defense, unfair competition, and wrongful behavior in general, particularly because transboundary data flows are governed by Art.

3.10 IPR, INTERNET AND LEGAL SYSTEM

In this regard, the points of contact that we propose for intellectual property rights on the internet lead to one legal system being applicable under three different viewpoints:

(1) Time: the person or legal entity entitled to use the intellectual property rights profits from their use but at the same time, incurs contractual or legal liability for its products or services (such as the strict liability standards of U.S. laws or the liability for risks of Article 1382 of the French Civil Code).[139]

(2) Geographical: The location where a dynamic act of wrongdoing causes financial damage is the victim's financial centre of gravity, or its principal business institution. This is also where the company's intellectual property rights are registered. Since intellectual property rights, unlike chattels, are not found in different jurisdictions, the loss cannot be located anywhere.

(3) Civil actions: A single regulatory scheme will extend to all damages claims (the success of which is often questionable due to the difficulties of proving missed profits) and benefit accounting under our plan (which an audit may more easily prove).

[139] WIPO, 'Overview of WIPO Panel Views on Selected UDRP Questions. WIPO Jurisprudential Overview 3.0' (3rd edn, 2017), para. 4.2

3.11 LET'S SUM UP

In this chapter, we have learned how various international treaties and conventions are regulating Private international law. Additionally, we have understood various related concepts like extra contractual liability, neighbouring right etc.

3.12FURTHER READING

- STROWEL & J.P. TRIAILLE, LE DROIT D'AUTEUR, DU LOGICIEL AU MULTIMÉDIA 386 (Brussels 1997); Lucas, supra note 23 at n° 96-97; Dutoit, supra note at 151-152.
- FRANÇOIS DESSEMONTET, INTERNET, LA PROPRIÉTÉ INTELLECTUELLE ET LE DROIT INTERNATIONAL PRIVÉ, Internet - Which Court Decides? Which Law Applies? 47-64 (1998)
- LUCAS & H.J. LUCAS, PROPRIÉTÉ LITTÉRAIRE ET ARTISTIQUE n° 976-980 (1994).
- François Dessemontet, L'enrichissementillégitimedans la propriétéintellectuelle, in RECHT UND WIRTSCHAFT HEUTE, FESTGABE FÜR PROFESSOR D. MAX KUMMER 191-214 (1980).

3.13 CHECK YOUR PROGRESS:POSSIBLE ANSWERS

1. **Define "country of origin".**

The definition of "country of origin" is central to the Berne Convention. This point of touch is responsible for determining whether a job is covered in other Member States (alternatively the nationality of the author). It also aids in the distinction between "domestic" and "international" works, which are works of the same origin as the forum and do not benefit from the Berne minimum requirements of security.

3.14 ACTIVITY

Explain Extra-contract liability in light of Private International law and Internet. (Word count 2000-2500)

Unit 4: INTELLECTUAL PROPERTY, CYBERSPACE AND INTERNATIONAL LAW

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 International conventions and territoriality

4.4 Territoriality on Intellectual property Right

4.5 Territoriality and National policy

4.6 Concluding remark

4.7 Let's sum up

4.8 Further reading

4.9 Check your progress: Possible Answers

4.10 Activity

4.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- The relationship between IPR, cyberspace, and its related aspects in cyber governance under International treaties.
- International treaties and conventions with respect to IPR.
- Various provisions of treaties and conventions governing the Internet laws and IPR.

4.2INTRODUCTION

The conflict of laws regulations was designed to resolve disagreements within territorial laws, also known as municipal laws. Since there are no independent national jurisdictions in cyberspace, territoriality is still present in the judicial system (with a few exceptions, such as the Panels adjudicating domain name disputes under the Internet Corporation for Assigned Names and Numbers ("ICANN") Policy or the World Trade Organization ("WTO") Dispute Resolution Body). As a result, conflict of authority remains a major concern in most fields of intellectual property. This has spurred calls for the establishment of a single European patent court. Beyond jurisdictional issues, however, harmonization of intellectual property law is not currently being pursued. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) represents just a sliver of agreement, and the World Intellectual Property Organization (WIPO) Treaties of 19964 only include copyright and adjacent rights. Many geographical differences also exist in trademark and trade name law, design law, copyright law, licensing law, unfair market law, and trade secrets law, as well as in the fields of broadcasting and publicity rights, to name only a few of the most important areas on the internet.[140]

As a result, we believe it is beyond time for a restatement of the dispute principles in intellectual property law. The Convention on the Law Applicable to Extracontractual Obligations may have accelerated the codification process in Europe, but it was squandered. As a result, another permanent body, such as the Hague Conference on Private International Law, will have to take on the responsibility. Since, as will be

[140] John M. Mrsich, Meeka Jun, "TermsYou Need to Know: Search Engines.": Description of how search engines work; terms used; and distinction among search engines, search directories, and search managers.

discussed further below, the current network of international conventions does not include a full collection of tools for settling such disputes, harmonization of conflict of laws rules is needed. The second section of this essay focuses on the internet's private international law in the area of intellectual property.

Cyberspace cannot be spoken of as a set of national jurisdictions. However, the inherently territorial existence of intellectual property rights precludes this. This chapter does not explore international laws that control cyberspace around the world since it focuses on intellectual property (for example, the domain name regulation system, the allocation system for internet protocol addresses). It also doesn't take into account how national and foreign legislation work in regards to cyberspace.[141]

4.3 INTERNATIONAL CONVENTIONS AND TERRITORIALITY

A. Scope of International Conventions on Intellectual Property

1) Areas Regulated by International Conventions

Patents, trademarks and geographic designations, trade names, designs and models, semi-conductor chips, copyright, neighbouring rights, plant variety, and trade secrets are all covered by existing treaties. Furthermore, Member States are required to ensure effective protection against unfair competition under the Paris Convention for the Protection of Industrial Property.

2) Minimum Rights

The multilateral Conventions provide intellectual property right holders with a minimum level of protection. Regardless of national legislation, all Member States can claim this minimum level of protection.

3) National Treatment

Discrimination against nationals of other Member States, as well as expatriates and refugees, is prohibited. As a result, any intellectual property right holder who is eligible to benefit from the Convention will be afforded the same level of protection in all Member States as a national of those countries. Most legal conflicts are

[141] Mark Sableman, Link Law: The Emerging Law of Internet Hyperlinks. The most recent and thorough examination of legal implications of hyperlink use on the Internet.A long but comprehensive look at the many legal arguments that can be made for and against users of hyperlinks.

suppressed by the equal protection of nationals and foreigners, combined with the minimum rights. When a national law differs from international standards, however, private international law issues arise. Although this deviation is justiciable before the WTO Dispute Resolution Body under the TRIPS Agreement, no other international mechanisms exist to ensure that Member States' legislation adheres to the international instruments' minimum rights. National governments have reacted in a variety of ways to the rapid advancement in technology. Conflicts of laws are becoming more common, owing to the fact that the major conventions have not been updated in the last three decades. In view of the Berne Convention, the issue of whether the framework of international treaties contains a set of guidelines for settling legal disputes will be discussed.

The other major intellectual property treaties, on the other hand, have the same effect on international law. Article 5 (2) of the Berne Convention guarantees the independence of the privileges granted to writers by national legislation. On first glance, this clause may cause one to conclude that the Convention establishes a dispute law. However, a thorough examination shows that Article 5(2) only prohibits discrimination against immigrants based on technicalities in their home country's rule. National copyright rules are "alone," which ensures that no deprivation of intellectual property rights under domestic legislation can be recognised by other Member States. That also ensures that no centralized infringement on the authenticity of copyrights for a certain work or subject matter is possible. Furthermore, contrary to popular belief in the nineteenth century, no reciprocity obligations can be enforced on immigrants requesting immunity from local courts. Even the Berne Convention, however, was unable to abolish all statutory reciprocity provisions in some contentious regions, such as copyright length, the "droit de suite" (right to an interest in resales), and the defense of applied arts.

4.4TERRITORIALITY OF INTELLECTUAL PROPERTY LAWS

First Sale Doctrine between Nations

Global obstacles to the importation of brand papers, proprietary books, and licensed materials are likely to be removed by the internet. International exhaustion is the e-commerce norm on the internet; anything accessed from a device is only subject to international exhaustion laws. However, for goods purchased on the internet and

sent by courier or postal, protection of local intellectual property rights is limited. We are seeing de facto international fatigue in motion. National courts, we believe, would be unable to implement a national exhaustion scheme for rights in conventional delivery systems in the long term, while e-commerce is focused on international exhaustion.[142]

Japan, Switzerland (except for patents), and the United States (at least for reimportation) are among the first countries to recognize international fatigue. The territorial solution to conflicts of law is inadequate in this case since the forum would define the first marketing abroad: was it rendered legally and with the consent of the intellectual property right holder? As a result, there is a strong extraterritorial bearing on the forum's legislation in operation (lexfori). The lexfori rarely has anything to do with the reality of the first marketing, with the exception of a few reimportation events. As a result, the court would often look at the copyright law (lexcontractus) that enabled the first merchant to bring the goods on the market to decide if the first sale was legal and done with the consent of the intellectual property right holder. Surprisingly, the legislation of the selling nation would be disregarded if it does not have enough protection for the issues at hand, such as drug patents. This approach is also possible outside of the TRIPS Agreement's signatories, since it is a matter of critical interest for national health programs. The "territoriality" of intellectual property rights does not tend to be the guiding concept in any case (application ofcontractus).

4.5 TERRITORIALITY AND NATIONAL POLICIES

The jurisdiction of Member States over their public health, economic growth, and cultural policies which cause national courts to exclusively extend the lexfori to intellectual property rights that are considered to play an important role in such policies, notwithstanding the fact that the international Conventions do not enforce absolute territoriality. It's worth noting that the Swiss Federal Tribunal would not recognize international fatigue in the field of patent law.[143] The reason for this is the economic consideration that while international fatigue prevails, a fair return on

[142]Lundstedt, L. (2016). Territoriality in Intellectual Property LawA compar ative study of the interpretation and operation of the territoriality principle in the resolution of transborder intellectual property infringement disputes with respect to international civil jurisdiction, applicable law and the territorial scope of application of substantive intellectual property law in the European Union and United States (PhD dissertation, Department of Law, Stockholm University). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-133470

[143]https://www.espon.eu/sites/default/files/attachments/ESPON_Policy_Brief_Territorial_dimension_of_future_policies.pdf

investment for patent holders is not assured because certain countries would not enable patent owners to set reasonably high prices.

In the United States, Professor William Patry has argued that, under Article I (8) of the United States Constitution, any work must meet the Copyright Act's originality requirements. Judge Kaplan of the Southern District of New York, on the other hand, and has responded that the acknowledgment of works covered under the lexoriginis stems from the United States Congress' Treaty Power. In addition, the United States Congress has ratified copyright conventions that provide for any connection to the country of origin.

There is one other point to remember that has yet to be discussed in the United States. The United States Congress has since adopted international human rights declarations, most specifically the International Covenant on Economic, Social, and Cultural Rights, in compliance with its Treaty Power. Intellectual property is protected under Article 15 paragraph 1 of this international treaty. The United States and other treaty partners cannot use their local rules to exclude themselves from their diplomatic obligations to uphold the treaty. Despite not being entitled to the value of the Berne Convention, the French courts correctly interpreted the Universal Declaration of Human Rights to allow Charlie Chaplin to seek immunity in France for his cinematographic works. A federal solution to intellectual property rights is ruled out by the prevalence of international commitments under the universal human rights doctrine. These rights are no longer the driving force behind national economic and cultural agendas. As a result, they are no longer subject to the whims of state governments. This also makes the United States' method of settling legal disputes by choosing the rule of the nation whose legislation seems to be the most relevant obsolete. Furthermore, as we can see, this approach is incompatible with the most current doctrine on conflict of laws.[144]

4.6CONCLUDING REMARK

The real issue for intellectual property rights holders in cyberspace is the protection of their rights. Although intellectual property rights are still territorial in nature, cyberspace must exist globally, and intellectual property security has been standardised by international treaties, especially the TRIPS Agreement. The

[144]ESPON. 2017a. “European Territorial Review: Territorial Cooperation for the Future of Europe.” https://www.espon.eu/european-territorial-review.

territoriality theory that defines intellectual property rights has also been loosened as a result of this standardization. The issue of territoriality of intellectual property rights will have to be addressed as part of any international cyberspace legislation. Any effort to regulate cyberspace and its relationship with intellectual property rights on an international level will pose the same legal and political challenges as any other international convention, as well as the need to create an international organization to track and police such a convention. However, in such a situation, international law may be used to control cyber threats and cyber war.

Outlining legal recommendations for internet infringements on intellectual property rights is just the first step. In certain cases, a straightforward test would not yield accurate results. When two or more experiments are used in parallel, the nearest relation is always discovered.

The reader should look back at previous publications and figure out why our series of tests was chosen. These assessments, according to some scholars, are not strictly dependent on the interpretation of the law of the receiving country. The policy is to favor a workable offer for goods and services under private law, as well as the use of intellectual property rights that can be monitored.

The enforcement of the legislation of the country of reception in a subsidiary capacity is not entirely ruled out. It can be used where a separate communication designates the same rule, for example, because the harm is obviously felt there and only there, or when it is a country shared by all sides. Where there is no worldwide distribution over a "Napster"-type relay, or uploading over a cell phone or other mobile devices in a different region, the legislation of the uploading country can also provide a very subsidiary examination. Finally, in extreme cases, the defendant's rule can be applied as the law of last resort.

In either test, the forum's public policy, such as any overreaching international policies, such as in antitrust zones, must be maintained. In the years to come, freedom of access, freedom of study, and freedom of speech, as well as droit moral and the security of intangible business properties, would generate enough tensions for dispute resolution laws to flourish.

4.7 LET’S SUM UP

In this chapter, we have learned how various international treaties and conventions

are regulating International law on IPR and cyberspace. Additionally, we have understood various related concepts like minimum right, National treatment etc. Besides, we have also analysed the territorial and extraterritorial policy formation along with its implication on cyberspace and in protection of rights under IPR.

4.8 FURTHER READING

- Rahmatian, Andreas (2008), 'Trade Marks and Human Rights', in: P. Torremans (ed.), Intellectual Property and Human Rights, Alphen aan den Rijn: Kluwer, pp. 335- 357
- Rahmatian, Andreas (2009), 'Dealing with rights in copyright-protected works: assignments and licences', in: E. Derclaye, Research Handbook on the Future of EU Copyright, Cheltenham: Edward Elgar, pp. 286-316
- Rahmatian, Andreas (2011), Copyright and Creativity. The Making of Property Rights in Creative Works, Cheltenham: Edward Elgar
- Rahmatian, Andreas (2013), 'Originality in UK Copyright Law: The Old "Skill and Labour" Doctrine Under Pressure', 44 International Review of Intellectual Property and Competition Law, 4-34
- Rosati, Eleonora (2013), 'Towards an EU-wide Copyright? (Judicial) pride and (legislative) prejudice', Intellectual Property Quarterly, 1, 47-68 Rousseau, Jean-Jacques (1968), The Social Contract, Maurice Cranston (ed.), London: Penguin
- Taubman, A. (2009), 'International Governance and the Internet', in: L. Edwards and Ch. Waelde (eds), Law and the Internet, 3rd ed, Oxford and Portland, Oregon: Hart Publishing, pp. 3-44
- Torremans, Paul (2005), 'Authorship, ownership of right and works created by employees: which law applies?', 27(6) European Intellectual Property Review, 220- 224
- Younes, Anan S. (2012), 'Trade Marks and Domain Names: Exploring the Inadequacy of Existing Protection for the Economic Value of Trade Marks', 34(12), European Intellectual Property Review, 847-852.

4.9 CHECK YOUR PROGRESS:POSSIBLE ANSWERS

1. What is minimum right?

The multilateral Conventions provide intellectual property right holders with a basic standard of security. Regardless of national law, all Member States will invoke this basic level of security.

2. What are the areas Regulated by International Conventions?

Patents, trademarks and geographic designations, brand names, designs and models, semi-conductor chips, copyright, neighbouring rights, plant diversity, and trade secrets are all covered under current treaties. Furthermore, Member States are expected to maintain adequate safeguards against unfair competition under the Paris Convention for the Protection of Industrial Property.

4.10 ACTIVITY

Explain Territoriality and National Policieslight of Private International law and cyber space. (Word count 2000-2500)

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

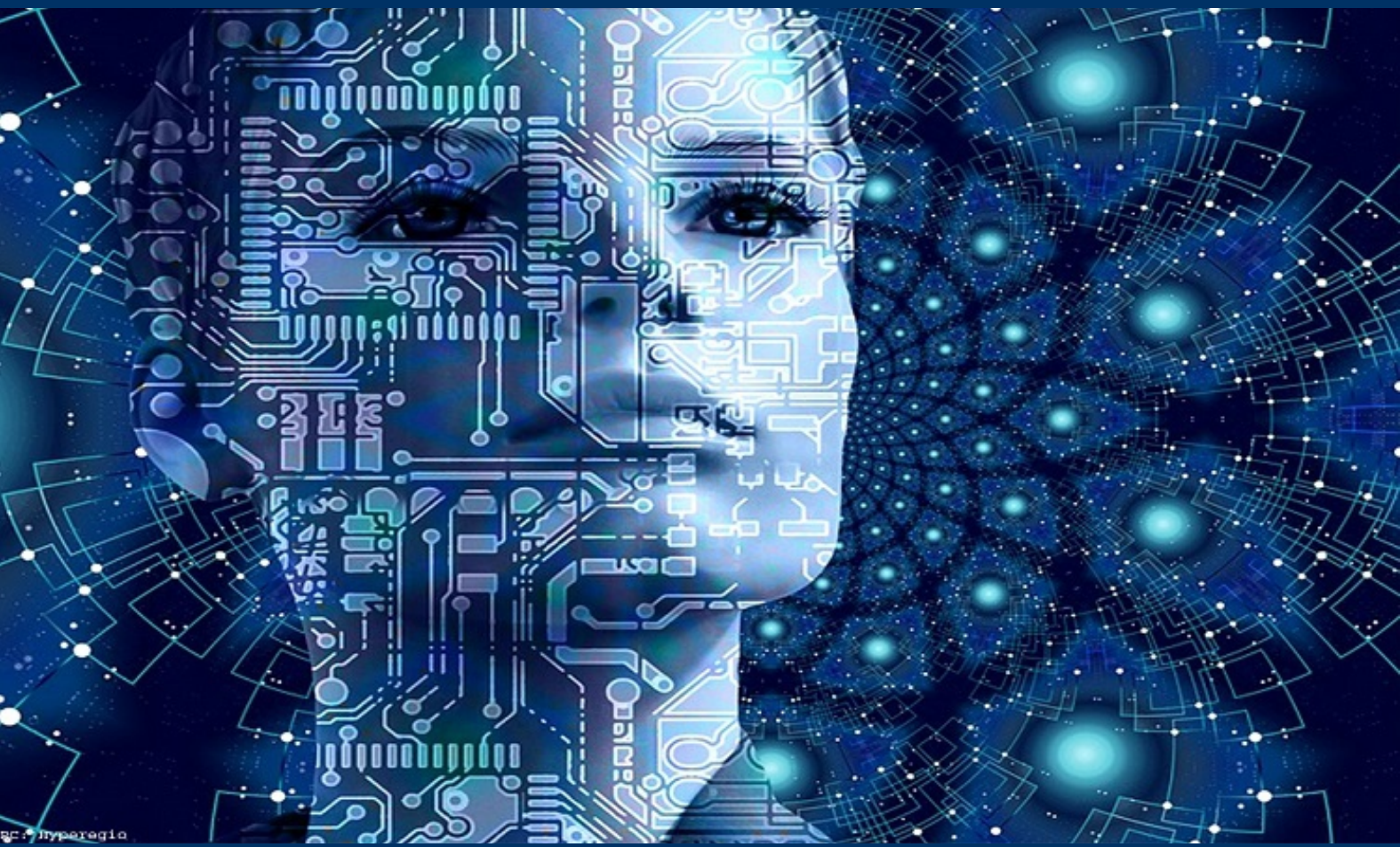
DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

BAOU
Education for All

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-203
Human Rights And Cyber Security Laws



Post Graduate Diploma in

Cyber Law

(PGDCL)

2021

Human Rights and Cyber Security Laws

Dr. Babasaheb Ambedkar Open University

Human Rights and Cyber Security Laws

Course Writer

Dr. DeeshaKhaire — Faculty of Law, Gujarat National Law University, Gandhinagar

Content Reviewer

Dr Peter Ladis — Faculty of Law, Chankaya National Law University, Patna, Bihar

Content Editor

Prof. (Dr.) Nilesh K. Modi — Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. 2021

ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr.Babasaheb Ambedkar Open University

PGDCL-203

Human Rights and Cyber Security Laws

Block-1: Cyber Security And Human Rights

UNIT-1
Introduction to Cyber Security And Human Rights 05

UNIT-2
International Trend In Ensuring Human Rights 11

UNIT-3
Case Study- USA 21

UNIT-4
Role of Civil Society 33

Block-2: Case Studies / Data Protection

UNIT-1
Equifax Data Breach: Case Study 41

UNIT-2
What's Up WithWhatsapp? A Transatlantic View On Privacy And Merger Enforcement In Digital Markets 48

UNIT-3
Facebook Data Theft In Indonesia 58

UNIT-4
Yahoo Data Breach 66

Block-3:Indian Laws And Cyber Security

UNIT-1
Privacy And Cyber Law 75

UNIT-2
Data Protection Bill 83

UNIT-3
Cyber Crimes And The Law: Evaluation Of The Information Technology Act, 2000 92

UNIT-4
Cyber Stalking And The Plight Of Women In India — A Legal Perspective 99

Block-4: Cyber Terrorism

UNIT-1
CyberTerrorism: An Analysis With An Indian Perspective 107

UNIT-2
The Cyber Terrorism Conundrum And 'Protected' Systems 114

UNIT-3
Countering Cyber Terrorism Effectively 120

UNIT-4
Assessing The Risks Of Cyber Terrorism, Cyber War And Other Cyber Threats 127

Block-1

CYBER SECURITY AND HUMAN RIGHTS

Unit 1:INTRODUCTION TO CYBER SECURITY AND HUMAN RIGHTS

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Adopting Cyber Security approaches which interrupt Human Rights

1.4 Applying a Human Rights Approach to Cyber Security

1.5 Privacy and Freedom of Expression

1.6 A Distributed-Governance Approach to Cyber Security

1.7 Roles of Stakeholders in Cyber security

1.8 Let's sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- what the cyber security approaches affecting human rights are.
- how to apply human rights approach to cyber security.
- privacy and freedom of expression.

1.2 INTRODUCTION

Cyber security is the frame of technologies, procedures and practices intended to defend networks, computers, programs and data from spasm, harm or unauthorized access. Elaborately it is the defence of computer systems from the stealing and injury to their hardware, software or information, as well as from commotion or misdirection of the amenities they deliver. Cyber security comprises governing physical entree to the hardware, as well as shielding alongside harm that may come via network entree, data and code injection. Also, owing to negligence by operators, whether intentional, accidental, IT security is vulnerable to being deceived into differing from protected measures through numerous approaches. The arena is of mounting reputation due to the cumulative dependence on computer systems and the Internet, wireless networks such as Bluetooth and Wi-Fi, the development of "smart" devices, comprising smartphones, televisions and tiny devices as part of the Internet of Things. Safeguarding cyber security necessitates synchronised pains through an information system.[1]

Human rights define rights intrinsic for every human, irrespective of race, gender, ethnic group, civilization, linguistic, religious conviction, or slightly extra position. Human rights comprise the right to lifespan and independence, freedom from bondage and torment, freedom of estimation and appearance, the right to effort and tutoring, and many more. Everybody is permitted to these rights, deprived of discernment. They are usually unstated as unchallengeable fundamental rights "to which a person is integrally permitted merely because she or he is a human being". They are pertinent ubiquitously and at each time in the intellect of being universal, and they are egalitarian in the wisdom of being the identical for everybody. They are observed as necessitating compassion and the rule of law and striking a compulsion on persons to esteem the human rights of others, and it is usually deliberated that they should not be taken away excluding as a result of due procedure based on precise environments.[2] If campaigners would like to triumph in contest for detainment in the Internet permitted and exposed, resulting in progressively vibrant which becomes necessity to disseminate them familiarly through the extents of cyber safety and cyber scrutiny. Worldwide state-funded cyber intelligence is assumed in delivery of the identical chronicles of cyber conflict and a cyber weapons contest; chronicles that came to existence castoff around in a few portions within the universe to embolden inhabitants for crafting on domestic permissions because of better

[1]Paul, Subrata&Mitra, Anirban& Mishra, Brojo.(2017). Cyber Security and Human Rights.CSI Communications. 41. 34-35.

[2]E A Fischer, "Cyber security issues and challenges: In brief," Congressional Research Service 2016, 2016.

wisdom of safety. Within India, we can't imagine for the entree of cellular devices else Internet acquaintances, comprising in cyber cafes, deprived of authorised documentation, and together ISPs and cyber cafes stand compulsory for preservation thorough records comprising operators' glancing antiquity. The fate chronicles which habitually escort these actions lure additional forte after identical actual development in the extent cyber-crime – where prevails numerous viruses besides added kinds of malevolent cypher in transmission, through a million persons flattering injured by cyber-crime daily. Therefore, although cyber security hasn't been a novel anxiety, over previous ages this originated in progressively govern besides ambition in Internet strategy besides supremacy program, in addition to worldwide strategy treatise extra sketchily. Cyber security approaches requisitely intended then applied by a manner such that it becomes reliable through global human rights regulation – besides frequently this was not the scenario, by way of realised in the investigation commands. On additional arenas, States establishes for being in arrears of coercions for instance cyber-attacks intended on human rights protectors' otherwise radical antagonism. It's consequently significant being wider human rights communal twitches appealing along with dissertations extra carefully, for unloading announced intimidations in addition to the hypothetical answers then safeguard human rights values remain supported midst cyber security showground also.

1.3ADOPTING CYBER SECURITY APPROACHES WHICH INTERRUPT HUMAN RIGHTS

With usage of encumbered, vague linguistic certainly elaborates extensive significances, by way of numerous governments consume imprecise interior besides exterior fears by way of influences to defend always better savings within cyber weapons besides bulk shadowing arrangements, also eternally superior administrative resistor in Internet plus own peoples. Owing to intellect in fright entrenched by cyber security accounts partakes troubled necessity of accurately also obviously authenticate probability besides features of hazards impending. Similarly assumed growth of imprint describing replies remain suitable besides genuine. Other threatening "security" actions include evolving supposed "Internet kill switches", confining usage of encryption, realising purifying besides obstructive apparatuses then announcing actual term strategies.[3] These methods frequently stance fears towards civic authorisations, so far these incline toward absence in jurisdictive omission in addition to communal information wherein magistrate on efficacy. Whereas boomingly that these advance safety, these commonly jeopardy obliterating the assistances which Internet carries.[4]

1.4APPLYING A HUMAN RIGHTS APPROACH TO CYBER SECURITY

The hearsays of UN Distinct Rapporteur delivers decent sympathetic about what way liberty of appearance smears. "International Principles on Communications

[3]Margaret Rouse, "Cyber security", http://whatis.techtarget.com/definition/ cyber security, retrieved: November, 2016.

[4]Gasser Morrie, "Building a Secure Computer System (PDF)". Van Nostrand Reinhold. Pp. 3.ISBN 0-442-23022-2.Retrieved on 6 September 2015.

Surveillance and Human Rights", labels chief philosophies of human rights method to cyber security equally defined by a collection of municipal civilization societies, business besides world-wide specialists.[5]

1.5PRIVACY AND FREEDOM OF EXPRESSION

Though additional human rights remain pertinent, two human rights specifically leads to the formation of structure chunks in rights- regarding tactics of cyber security. First comes right to privacy, freedom in keeping everyone's information and communiqué left after predatory judgements of management, industries or extra peoples. Right to privacy becomes an essential constituent over expansion of a people specific safety strategy. Though it's inadequate still because it unconsumed the necessities aimed at existence protected operational in method being elaborated. Privacy is inhibited when someone becomes deprived of the privacy in transportations or mechanism concluded evidence around them. Over valuation in cyber security strategies identical physique willingly specified over functional pleasure with every inhabitants of the right to freedom of countenance. Additional dominant right, freedom of countenance, inhibited whenever an act averts somebody after looking for, getting or communicating somewhat appearance except those could be legally imperfect, besides movements which "anxieties", i.e. disheartens else constrains, which countenance.

1.6A DISTRIBUTED-GOVERNANCE APPROACH TO CYBER SECURITY

Though cyber threats are frequently actual, present dissertation hereby consuming a diversity of undesirable influences, affecting the Internet domination programme absent after making an available and allowing atmosphere and concerning discovery novel, and progressively federal, systems of knowledge and controller. An important characteristic of the cyber security dissertation exists in the idea of an influential besides caring Public provided that his peoples through safety, similar to the pre-Internet stage. Nonetheless this account takes a pew nervously along realism of Internet's behaviour that stands as world-wide network of evidence that is unto a great amount for indicators of private segment. Neither fears nor explanations are consequently by way of effortlessly distinct, positioned before bounded as similar to past. Through a disseminated methodology, supremacy preparations purposefully consensus numerous performers precise parts besides errands at cyber security field, nonetheless being accomplished in a manner when none solitary performers are capable of regulating this field except the others approve and cooperate.[6] The other metier of such a tactic becomes permit users to redo the distinction between the operators as an important performer in this expanse. Certainly, because intimidations remain rapidly changeable over Internet atmosphere, finest resistance will frequently be consuming knowledgeable operators can themselves undertake bright conclusions; although present governance preparations consist of slight area

[5]Nickel, James, "Human Rights". The Stanford Encyclopedia of Philosophy (Fall 2010 ed.).

[6]Anja Kovacs and Dixie Hawtin, "Cyber Security and Online Human Rights" Internet Democracy Project, Global Partners and Associates, November 2017.

for it. Totalling, in pointing multiple-layers of payments and stabilities, this tactic can be additional probable in sustenance of human rights.

1.7ROLES OF STAKEHOLDERS IN CYBER SECURITY

In talking about the multilateral and multi-stakeholder ways in which cyber security is addressed, it is important to understand what role different stakeholders play in these discussions. Ideally, governments, the private sector, civil society, and the technical community would all play equal roles in creating and implementing cyber security policies and decisions, but realistically this isn't always the case. Traditionally, governments play the primary role in creating the public policies and laws that regulate and determine cyber security measures domestically, sometimes with non-governmental input, but usually from private cyber security firms or industry. In addition, governments are also capable of launching and supporting cyberattacks of their own against other countries, and they are the only stakeholder guaranteed a say in the ITU and other international multilateral bodies. On the international stage, a handful of governments (previously mentioned) have pushed for increasing the role of governments and intergovernmental organisations in cyber security. Private sector companies, including ISPs and the IT sector are crucial because of their role in creating and maintaining the technologies (computers, tablets, etc.) on which cyber security issues arise. Governments often consult these companies when making public policy decisions in order to ensure that cyber security standards can be applied to various technologies. At the same time, the number of cyber security firms in the private sector is quickly growing, and they often profit from strict cyber security policies. Similar to private sector companies, the technical community has the technical expertise and understanding of the Internet and is often cited by governments when developing cyber security policies. The technical community, including the Internet Engineering Taskforce also works independent of governments and politically-motivated cyber security measures to help ensure the security of the Internet's critical infrastructure. Similar to other areas of Internet governance, civil society's role in cyber security has just begun to take off in recent years. On the one hand, civil society groups have pushed for further inclusion at international discussions and domestic policymaking meetings, but others are calling for civil society to create their own positive agenda for cyber security policy and norm making. Civil society has a unique role in being able to advocate for cyber security policies from a human rights-based approach. In 2011, CitizenLab developed a report outlining the possible role for civil society in cyber security, and in 2013, the Association for Progressive Communications created a similar agenda. Both reports emphasise the importance of civil society in bringing to light human rights considerations in all cyber security related discussions, but also address the need for civil society to call for evidence based cyber security decisions and practices.

1.8 LET'S SUM UP

The intention of this chapter is to highlight some key developments relating to the current climate around cyber security and human rights in order to set the stage for a dynamic and in-depth discussion.

1.9FURTHER READING

- Selma Dilek, HüseyinÇakır and Mustafa Aydın, ”Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015.
- Margaret Rouse, “Cyber security”, http://whatis.techtarget.com/definition/ cyber security, retrieved: November, 2016.
- Gasser Morrie, “Building a Secure Computer System (PDF)”. Van Nostrand Reinhold. Pp. 3. ISBN 0-442-23022-2. Retrieved on 6 September 2015.
- Rouse Margaret, “Social engineering definition”. TechTarget. Retrieved on 6 September 2015.
- James Nickel, Thomas Pogge, M.B.E. Smith, and Leif Wenar, “Stanford Encyclopaedia of Philosophy, Human Rights “, December 13, 2013, Retrieved on August 14, 2014.
- Nickel, James, “Human Rights”. The Stanford Encyclopaedia of Philosophy (Fall 2010 ed.).
- The United Nations, Office of the High Commissioner of Human Rights, What are human rights? http:// www.ohchr.org/en/issues/pages/ whatarehumanrights.aspx, Retrieved August 14, 2014.

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyber security?**

   Cyber security is the frame of technologies, procedures and practices intended to defend networks, computers, programs and data from spasm, harm or unauthorized access**.**

2. **What are Human Rights?**

   Human rights define rights intrinsic for every human, irrespective of race, gender, ethnic group, civilization, linguistic, religious conviction, or slightly extra position.

1.11 ACTIVITY

1. Discuss about the intermingled relations between cyber security and human rights along with your opinion on the same. (1500-2000 words)

2

Unit 2: INTERNATIONAL TREND IN ENSURING HUMAN RIGHTS

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Deconstructing Cyber Security

2.4 Human Rights violation in Cyber Space

2.5 A Human-Centric Perspective on Cyber Security

2.6 Let’s sum up

2.7 Further reading

2.8 Check your progress: Possible Answers

2.9 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- cyber security in the International scenario
- human rights' violation of cyber space
- cyber security in a human centric perspective

2.2 INTRODUCTION

The evolution of cyberspace has had an influence on nearly every area of human life over the last two decades. Cyberspace's growth in the tempo, frequency, and variety of interactions has changed the way communities communicate, businesses provide services, and individuals are regulated. Big Data and the Internet of Things (IOT) are now having an effect on a wide variety of social events. The cyber realm is now posing an increasing range of security challenges. Critical national infrastructures are vulnerable to cyberattacks, and cyber-espionage and cybercrime pose a threat to the global economy. Worms, malware, advanced Distributed Denial of Service (DDoS) attacks, and spam have lost billions of dollars to the global economy. Cyber attacks on Estonia's online banking infrastructure and the use of the Stuxnet worm to damage Iran's nuclear program show how important cyberspace is for national security.[7] States have naturally identified cyberspace as a modern area of war in their military and security doctrines. The concept of national security dominates the electronic security conversation. This pattern can be seen in the publication of national security strategies and official reports, the creation of cyber-commands and Computer Emergency Response Teams (CERTS), the amount of money spending to protect cyberspace, and the talk of a cyber-arms race. While this policy is justified to a significant degree, it is still flawed in that it ignores the human rights of approximately 2.7 billion Internet users. The evolution of Internet filtering tactics, as well as Edward Snowden's disclosures regarding the US National Security Agency's (NSA) global surveillance program, have shown that Internet freedom, anonymity, and personal data are continuously under threat. Interception and monitoring of citizen communications are commonplace. As a result, cyber defense can not only counter challenges to the state and private sector, but also (if not first and foremost) human needs.

2.3DECONSTRUCTING CYBER SECURITY

Cyberspace has become an inseparable part of human civilization, and our reliance on its technology is becoming all the time. When addressing a contentious topic like cyber defense, the reader should keep the following in mind. First and foremost, there is no explicit understanding of what constitutes cyber defense, owing in part to

[7] Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance by Andrew N. Liaropoulos (University of Piraeus, Greece)

the lack of a widely agreed definition of cyberspace.[8] Cyberspace is a concept with a nebulous meaning that is commonly used as a synonym for the Internet or the World Wide Web. Daniel Kuehl describes cyberspace as "a global realm within the knowledge world whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to generate, store, alter, share, and manipulate information through interdependent and interconnected networks using information communication technologies," according to one common concept.[9]When it comes to cyber security, the key issue is whether one sees cyberspace as a global network involving only hardware, applications, and information systems, or as a network involving individuals and the vast variety of social activities that take place within it. The second problem is that there are several words used to characterize various facets of cyber security. Scholars and government officials frequently use terminology like information security, ICT security, network security, Internet security, and essential information technology privacy. This language encompasses a wide range of risk categories and levels in cyberspace, posing valid questions regarding the referent object of cyber protection. The fact that all of the aforementioned words take on different meanings when put in a political context adds to the semantic complexity. In each nation, the conceptions of state control in cyberspace, approaches to solving the attribution dilemma, methods of establishing cyber deterrence, and the fine line between information security and internet censorship differ. States will have diverse interests when it comes to meeting the security needs of government, business, and people in the cyber domain because they have distinct national goals and capacities in cyberspace.[10] National security interests in cyberspace may include not only combating hackers, criminals, terrorists, or other governments, but also controlling or even manipulating knowledge traffic and records, depending on the situation. The final point to consider, and one that is often overlooked, is that security was not a top priority in the early stages of cyberspace growth. Its architecture was built on the principles of simplicity and transparency rather than protection and durability.

The aim of the original design of APRANET and the subsequent information architecture was to build an open environment in which researchers could exchange ideas without being constrained by time or distance. The Internet's promise was to be a place where people could openly communicate, monitor news, and exchange knowledge and ideas. Any national security agenda should aim to provide a safe atmosphere for its people. Given the fact that modern democracies depend on the operation of ICTs, it is only natural to believe that one of the goals of any national cyber security strategy will be to provide a safe cyber environment for its people. This goal translates into the defense of vital national infrastructures in policy terms.[11] As a result, states are building offensive and defensive cyber-weapons in order to protect their cyber assets. Offense-defence theory, deterrent theory, center of gravity, arms race, and doom scenarios are all included in the related security and military doctrines. States view cyber defense as a zero-sum game because they

[8]Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and ApuKapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.ACM, Seoul, 3523–3532.

[9]Jeffrey Bardzell and ShaowenBardzell. 2016. Humanistic HCI. Interactions 33, 2 (2016), 20–29.

[10]Matt Bishop. 2018. Computer security: Art and science. Addison-Wesley, Boston.

[11]Matt Blaze. 2019. Testimony of Prof. Matt Blaze. https://www.mattblaze.org/papers/blaze-homelandsecurity-20191119.pdf

emphasize the technological and military dimensions of cyberspace rather than the socio-political ones. States are caught in a classic security challenge in their attempts to protect cyberspace. The chaos that remains in the world community is the source of this security problem. States unconsciously make other states feel less comfortable by attempting to improve their states' defense, typically by enhancing military capability. As a consequence, there is a never-ending cycle of security-insecurity. This conundrum can be deconstructed into a two-level strategic game.[12]

In the most basic level, the perception question arises from a lack of knowledge regarding the motivations, intentions, and capacities of other actors. Decision-makers at the second level must decide how to react. The solution dilemma does not begin until the understanding dilemma has been resolved. Uncertainty and distrust are prevalent in cyberspace, much as they are in the physical world. States are concerned about other parties' intentions and cyber technologies, so they build offensive and defensive cyber-weapons. More instability is provided because there is little to deter states from trespassing on the digital boundaries of other states. The dilemma of meaning and the dilemma of answer result from this spiral of uncertainty. The current approach to cyber security, on both the public and private levels, is focused on the defense of vital national infrastructures (public and private) rather than citizen rights. Cyber attacks against information infrastructures, as well as worms and viruses, are viewed as cyber threats rather than breaches of privacy and/or freedom of speech at the interpretation stage. The 'human' factor as a security target is not only downplayed, but it is also included in the threat continuum (hackers, for instance). A possible national (cyber) challenge is anybody with a device linked to the Internet and the requisite technological skills. Similarly, at the response stage, the aim is to secure vital national infrastructures rather than people's right to obtain access to cyberspace services and use them according to their needs and desires. The cyber security problem not only causes a vortex of instability between states on a global scale, but it also has negative consequences within states.

Cyber technologies built to protect and safeguard a country's vital national resources are also used against its own people. Citizens are caught in a "liberty vs protection" paradox, where they must give up civil rights in exchange for greater security. In other words, policymakers use cyber protection as an excuse to track, manipulate, and attack web information. The aim of the Cyber Intelligence Sharing and Protection Act (CISPA), for example, was to allow the US government and businesses to defend the nation's information technology from international cyber attacks. CISPA allows businesses to give the government confidential consumer details without a warrant. Private businesses gather large amounts of personal data (customer preferences), and policymakers can access these private databanks with a single click. Another example is the use of cryptography to safeguard our personal information when communicating. The prohibition of encrypted messages could be seen as a violation of both the right to privacy and online anonymity, but it could also be justified for national security reasons.

Encryption, as a result of technology, is neither good nor evil. Citizens and terrorists both use the same encryption that shields governments and companies. Citizens are not the winners, but rather the casualties, of national cyber protection measures in

[12]Cerf, V. (2011).The Battle for Internet Openness.IEEE Internet Computing. 15 (5), 104

such situations. The cyber arms race has resulted in a reduction in Internet freedom within states. Filtering systems that block access to specific websites, encryption restrictions, the invention of Internet kill switches, and monitoring systems to track online activity are all tactics that have a significant impact on privacy, confidentiality, and therefore security. The use of counter-censorship tactics during the Arab Spring and the Snowden disclosures regarding the NSA's global surveillance in the name of counterterrorism are also dramatic illustrations of cyberspace's dark side.

2.4HUMAN RIGHTS VIOLATIONS IN CYBERSPACE

Individuals around the world are constantly at risk of human rights violations related to cyberspace. Governments employ a variety of measures that violate freedom of expression and the right to privacy, like targeting dissident voices, internet filtering practises or even disconnecting access to ICTs. Below are some examples of cyber surveillance and online censorship. In 2009, the re-election in Iran of President Mahmoud Ahmadinejad led to a social uprising of young Iranians, claiming that the votes were manipulated and calling for an investigation on the voting fraud. Iranians used social media, mainly Twitter to disseminate information about the protests. During the social uprising in Iran, social networking sites were blocked by the regime and the intelligence and security services managed to identify and close down the activities of those promoting dissent. In Tunisia, the self-immolation of the 26-year-old fruit and vegetable seller Mohamed Bouazizi on 17 December 2010, triggered nationwide protests against the oppressive government of Ben Ali.[13] The regime responded by disrupting the flow of information in social media, by hacking e-mail and Facebook accounts. Likewise in Egypt, the protesters demanded Mubarak's resignation and the reinstitution of democracy. The protesters used social media not only to spread the message, but also to share content like online maps and encryption techniques. The regime soon realized the importance of social media for its political survival and intensified the online censorship.

The Egyptian police monitored social networks, email accounts of dissidents as well as Skype and arrested dissidents that were responsible for coordinating the protests. In late January 2011, the regime, in a desperate move to control the information flow, decided to cut off access to Internet for a few days. In January 2010, Google announced that a computer attack originating from China had penetrated its corporate infrastructure and stolen information from its computers, most likely source code. The attacks also targeted Gmail accounts of some human rights activists and infiltrated the networks of 33 companies. A recent study by the European Parliament titled 'Surveillance and censorship: The impact of technologies on human rights' mentions a variety of measures that states use in order to control the information flow. One such measure that aims to discourage citizens from creating their own blogs and expressing their opinions, is the mandatory registration of online media with pubic authority. In Saudi Arabia, only citizens that can produce 'documents testifying to good conduct' and with a high school diploma are allowed to start their own blog or website.

Likewise in Belarus, websites must register using the national domain and be hosted on national territory. Another option is the control of the telecommunications industry

[13]Liaropoulos, Andrew. "In Search of a Social Contract for Cybersecurity." European Conference on Cyber Warfare and Security, Academic Conferences International Limited, July 2019, p. 282.

by governments. China has developed a set of technical solutions like the Great Firewall to block online content from foreign servers. Pakistan is blocking thousands of websites as part of its policies against terrorism, blasphemy and pornography. In Turkey, Google and Facebook were asked to remove political content during the Gezi park protests in 2013 and Twitter and YouTube were blocked before the elections in March 2014. The Snowden revelations about the mass surveillance programs conducted by the 'Five Eyes' (USA, UK, Canada, Australia and New Zealand) demonstrated the magnitude of human rights violations in the digital sphere and the rise of the surveillance state. In particular, the PRISM program enabled NSA to have direct access to the servers of Apple, Facebook, Google, Microsoft, Skype, Yahoo, Twitter and YouTube. The working relationship between intelligence and security agencies on the one hand and private sector one the other hand, raises a number of ethical and legal questions regarding electronic surveillance, citizen privacy and national security.

The Snowden disclosures also accentuated the role of Big Data. The capabilities that Big Data practices offer, are transforming the way surveillance is conducted. Personal data are not collected for limited and transparent purposes, whether that is public safety or national security. The traditional police and intelligence methods of identifying targets and then collecting data was reversed with Big Data. Instead, evidence is still being gathered until a decision is made about the full scope of their current and future applications. Big Data algorithms, according to the logic, would help us to predict behaviours and events. Big Data analysis' pre-emptive reasoning is undermining current regulatory processes that are built on an after-the-fact scheme of fines and punishments.[14]

2.5A HUMAN-CENTRIC PERSPECTIVE ON CYBER SECURITY

Based on the above review, it can be concluded that existing cyber security strategies do not provide consumers with a safe cyberspace. A quick glance at the press and official papers demonstrates that cyberspace is not a secure environment. In stark contrast to early expectations, the Internet is increasingly becoming a weapon of totalitarian rule. In the 1990s, the so-called cyber-utopians were unable to anticipate how effective the Internet would be for propaganda, how states (both democratic and authoritarian) would use cyberspace for surveillance, or how sophisticated censorship would become.[15]It is unfounded to believe that technology (and therefore ICT) empowers citizens rather than state oppressors. On the Internet, maintaining anonymity seems to be difficult. Governments and companies are amassing vast amounts of personal information. Users' accounts are detailed on search engines and online social networking platforms like Google and Facebook, and mobile phone providers use GPS systems to monitor and find their users. All private data is stored, and people's online behaviour and consumer habits are correlated and passed from companies to governments, most of the time without the knowledge and consent of the users. The transparency reports of Google, Microsoft

[14]Surveillance, Snowden, and Big Data: Capacitieshttps://journals.sagepub.com/doi/full/10.1177/2053951714541861

[15]Liaropoulos, Andrew. "Cyber-Security: A Human-Centric Approach." European Conference on Cyber Warfare and Security, Academic Conferences International Limited, July 2015, p. 189.

and Twitter show that most of the requests to companies for user data originate from liberal democracies. Companies who make tools for social network mining, mobile phone monitoring, and data manipulation are signing deals with democracies and authoritarian regimes all over the world. The cyber security industry, as the military-industrial complex before it, is amplifying the arms race in cyberspace and thereby empowering the cyber surveillance state. A issue that eventually arises is whether a different approach to cyber security will help us to avoid the cyber security challenge while still ensuring human rights safety.[16] Would an anthropocentric approach be useful in addressing the need of humans in the cyber realm? Safeguarding human needs in any domain, including cyberspace, raises once more the question about the meaning of security. The term 'security' is usually associated with the absence of threats to scarce values which might threaten the survival of the referent object.[17]

Security can be seen in both a positive and negative light. Security is described as the absence of threats to core human values in the negative sense, and policies and practices that protect and enable people to exercise their rights openly and safely in the positive sense. It is this positive conception of security that seems to be undervalued in the current cyber security discourse. States have historically viewed security in negative terms; and, thus, they also view cyber security as mainly the absence of harm. "Cyber security strategies should not only play a protective role, but also a supporting role, by ultimately placing the empowerment and well-being of people at their center," Kovacs and Hawtin argue. What we want people to be able to do is to be fearless as long as they honour the human rights of others."Human rights include freedom of expression, freedom of speech, freedom of thought, and the right to privacy, as protected by the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). It's worth noting that the UN Human Rights Council agreed in July 2012 that people's online rights must be secured in the same way that they are offline (Green & Rossini, 2015, p. 8). So how can states strike a balance between the protection of critical information infrastructure and data flows on the one hand and the right to privacy and online anonymity on the other? And who will be responsible for protecting, implementing and enforcing human rights in cyberspace?

In response to these questions, we need to note the following. First, the governance of cyberspace is still under construction. In particular, cyberspace lacks a single forum or international organization that is responsible for regulating its activities. As a result, governance is spread throughout technical standard setting fora, private sector organizations, civil society groups, states and international organizations.[18] Governance ranges from developing norms and codes of conduct, to signing international treaties and imposing regulations. Over the past years, there have been attempts both at the national and the international level to address human rights' concerns in cyberspace. States have passed laws and taken initiatives to counter cyber threats, but an international treaty that would regulate activities in cyberspace is still absent.

Since 2010, the Groups of Governmental Experts (GCEs) have been appointed by the UN General Assembly to report on the nature of cyber threats and their implications for national and international security. In their reports, the GCEs

[16]Bajaj, K. (2014) 'Cyberspace: Post Snowden', Strategic Analysis, Vol.38, No.4, pp.582-587

[17]Jervis, R. (1978) 'Cooperation under the Security Dilemma', World Politics, Vol.30, No.2, pp.167-214.

[18]Dilipraj, E. (2014) 'Internet Governance: The shift from monopoly to multi-party', National Defence and Aerospace Power, 99/14.

emphasized that states have to respect human rights and fundamental freedoms when addressing cyber security issues. Likewise, in 2013, the European Commission adopted the 'Cyber security strategy of the European Union: an open, safe and secure cyberspace' which states that EU's core values apply as much in the digital as in the physical world and that cyber security is only effective when based on fundamental rights and freedoms.

Despite the above positive developments, there is still no law enforcement mechanism that can ensure the protection of human rights in cyberspace. For example, there is no universal consensus on what constitutes personal data in cyberspace. The EU treats IP addresses as part of personal data, whereas the US does not. Likewise, in terms of data privacy, the EU applies a strict and top-down regulation system, where governments play a leading role, whereas the US relies more on industry self-regulation mechanisms. Another point to consider regarding the protection of human rights in cyberspace is the future demographic trends. Nowadays, only 30% of world population has regular access to the Internet.[19] The next billions of Internet users are coming from states in the Global South that embrace a Westphalian understanding of state and national security. Many of these states have authoritarian and autocratic regimes that have already developed cyber surveillance programs, at the expense of human rights. Pushing the global agenda for a human-centric understanding of cyber security, is not a priority for these states. Second, in the absence of global governance, the state is the sole player with the authority and capacity to meet human needs. This isn't meant to minimize the relevance of a human-centered approach to cyber security; rather, it's meant to put the debate in perspective. International and private players (international government and civil society) can be included in this sense, but states cannot be excluded. The defense of a state's territories, sovereignty, and people is described as national security. That notion expresses the reality of the pre-Internet era. Cyberspace is different from the other physical domains (land, sea, air, and space) against which states have to safeguard. Cyberspace is a transnational domain in which states are trying to overcome the border paradox and exercise their sovereignty.[20]

The oxymoron is that states have a responsibility to protect their people in cyberspace, but they make them feel vulnerable by infringing their online human rights. Because of the potential for violence, framing the defense of human rights in cyberspace as a national security problem may be counterproductive. States must recognize that people should be able to take advantage of the advantages of cyberspace rather than being the targets of widespread and illegal cyber surveillance. Protecting privacy and freedom of speech, as well as limiting unjustified public-private exchange of personal data, should be included on policymakers' electronic security agendas.

2.6 LET'S SUM UP

Various fields have addressed cyber defense. The controversy about the essence of cyber security has been enriched by information technology specialists, judges,

[19]Hare, F. (2010) The Cyber Threat to National Security: Why Can't we Agree?, in Czosseck C. &Podins, K. eds, 2nd International Conference on Cyber Conflict Proceedings, NATO CCD COE Publications, Tallinn.

[20]Mordini, E. (2014) 'Considering the Human Implications of New and Emerging Technologies in the Area of Human Security', Science and Engineering Ethics, Vol.20, Issue 3, pp.617-638.

strategists, and state leaders. State-centricity is the prevailing theme, regardless of its theoretical basis. The new cyber security strategy is ineffective and completely irrelevant, if not aggressive, to people's needs. States are producing cyber (in) security both at the international system and among sub-state players, rather than making cyberspace more stable. The rights of governments have overwhelmed the interests of citizens in this situation, as they have in many others in the past. Indeed, electronic weapons designed to protect a nation's cyber properties are being used against its own civilians. Breaking the "cyber security paradox" and finding a balance between national cyber policy on the one hand and privacy, secrecy, and freedom of expression on the other are enormous challenges. The risks that the idea of a "surveillance regime" entails are not recent.

The fear is that cyberspace will transform this sinister metaphor into reality, or has already done so. Anonymity is vanishing in the era of Big Data and the Internet of Things. By personal ads, companies are using meta-data to form marketing campaigns. Monitoring the entire spectrum of human actions in the digital realm is critical to the role of national security and intelligence services. While the securing of cyberspace is unavoidable, the shape that cyber defense will take in the immediate future is not. In fact, the current securitization of cyberspace is intertwined with the securitization of every part of our lives. Shifting the narrative to human rights is just the first step in ensuring internet users' safety. Securing human interests in a domain devoid of meaningful governance and blurring the boundaries between national and international, public and private, is a conundrum wrapped in a mystery.

2.7FURTHER READING

- Cropf, R., & Bagwell, T. (Eds.). (2016). Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance.
- Dunn Cavelty, M. (2012). The militarization of cyberspace: why less may be better. In C. Czosseck, R. Ottis& K. Ziolkowski (Eds.), Proceedings of the 4th International Conference on Cyber Conflict (pp.141-154). Tallinn, Estonia: CCD COE Publications.
- Betz, D., & Stevens, T. (2011). Cyberspace and the state: toward a strategy for cyber-power. Adelphi Paper 424. Oxfordshire, UK: IISS & Routledge.
- Booth, K., & Wheeler, N. (2008). The security dilemma: fear, cooperation and trust in world politics. New York, USA: Palgrave.
- Brantly, A. F. (2014). The cyber losers. Democracy and Security, 10(2), 132–155.

2.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is cyberspace?**

Cyberspace is a global realm within the knowledge environment identified by the use of electronics and the electromagnetic spectrum to build, store, alter, share, and manipulate information through interdependent and interconnected networks using information communication technologies.

2.9 ACTIVITY

Analyse the intricacies of cyberspace and its effect on human rights. (1500-2000 words)

3

Unit 3: CASE STUDY- USA

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Cyber Security as Human Rights Issue

3.4 Defense Advanced Research Projects Agency (DARPA)

3.5 The Threat Environment

3.6 New Strategy

3.7 Let’s sum up

3.8 Further reading

3.9 Check your progress: Possible Answers

3.10 Activity

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- cyber security as human rights issue
- Defense Advanced Research Projects Agency (DARPA)
- threat environment of cyberwarfare

3.2 INTRODUCTION

There is no universal definition of cyber security; however, the definition developed by the “Internet Free and Secure” working group of the Freedom Online Coalition (FOC), which was composed of technologists, human rights experts and government, is instructive. Inspired by the International Organization for Standardization 27000 standard, the FOC working group defines cyber security as “the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.”[21]

3.3 CYBER SECURITY AS HUMAN RIGHTS ISSUE

3.3.1 Why cyber security is a human rights issue

Using the FOC definition of cyber security as a basis, it is easy to see how threats to cyber security – or cyber insecurity – can be human rights violations. The denial of availability of information and its underlying infrastructure, in the form of network shutdowns, for example, violates a wide range of rights, including by unduly restricting access to information and the ability of people to express themselves, peacefully assemble and associate, as well as enjoy a range of economic, social and cultural rights. In 2018,196 internet shutdown were documented in 68 countries.

There are countless examples of the confidentiality of information being compromised, whether through data breaches for financial gain, mass government surveillance or targeted attacks on human rights defenders or journalists, in violation of the right to privacy, among other rights. Breaches of the confidentiality of

[21]https://www.apc.org/en/news/why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

communications through surveillance is linked to severe human rights violations, like detention, torture and extrajudicial killings. An example of a particularly egregious case is the surveillance of Saudi dissident Omar Abdulaziz, which contributed to the extrajudicial execution of Saudi journalist Jamal Khashoggi. According to a lawsuit, Abdulaziz's cell phone was targeted by the Saudi Arabian government with spyware, compromising the confidentiality of his communications with Khashoggi about opposition projects in the months leading up to Khashoggi's killing.

While most people are likely to experience some form of cyber insecurity in their lifetime, even people for whom meaningful access to the internet is a challenge, cyber insecurity is not experienced evenly by everyone. Human rights defenders, journalists, and people in positions of marginalisation or vulnerability, because of their religion, ethnicity, sexual orientation or gender identity, for example, can experience particular risk. For example, they are more likely to be targeted by government or lateral surveillance, and the consequences of more broad threats like data breaches or network shutdowns are often more severe for them because of their location within society.

As more people and devices are connected, the risks that come with cyber insecurity will only increase. Unfortunately, governments are either not centring cyber security discussions on human rights, or worse, they are using cyber security as an excuse to exercise more control over the internet.

3.3.2 The securitisation of "cyber"

The development of laws, policy and norms on cyber security tends to take place in highly opaque, securitised settings without the benefit of civil society input or human rights expertise. This runs counter to the multistakeholder approach to internet governance, which relies on the full involvement of governments, the private sector, civil society and international organisations. Critically, this approach excludes the expertise and monitoring required to protect human rights. Often, cyber security discussions happen in the confines of intelligence services, or other government or military agencies that are not subject to public scrutiny or oversight. Cyber security is also sometimes equated with national security, which is characterised as a sacred sphere in which governments can do whatever they want and without public scrutiny, much less oversight. As a result, cyber security law, practices and policies are often divorced from a human rights framework, and susceptible to abuse of power.

3.3.3 International cyber security debates miss the mark

It is well established that international human rights law applies to digital technologies. However, when it comes to cyber security, international human rights law is not central to discussions, if a factor at all. This is partially due to the fact that international discussions on cyber security predominantly respond to the issue of state-on-state attacks and fall under the rubric of international security and disarmament. Nonetheless, the tenor of these discussions, and the norms that stem from them, have implications for how states approach cyber security at the national level. Of particular concern are efforts by the Shanghai Cooperation Organization (SCO), which for years has been working to advance the concept of extending national extending national sovereignty and information control in cyberspace.

The UN has held since 2013 that international law, which includes international humanitarian law and international human rights law, applies in cyberspace. In 2015, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security further elaborated that respect for human rights and fundamental freedoms is seen as being “of central importance” and recommended that states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age.

While the international community has gotten stuck on how international law applies in cyberspace, the focus has primarily been on international humanitarian law. This approach is flawed for several reasons. First, international humanitarian law applies only in times of armed conflict, whereas international human rights law applies at all times (in peace and war). Given that most of the types of cyber insecurity are experienced during peacetime (or at least in the absence of a declared cyber war), international human rights law is more frequently the applicable framework. Second, and relatedly, centring debates on international humanitarian law may somehow advance the belief that states are in a perpetual cyber conflict, leading to an escalation in cyber attacks. Third, international humanitarian law is a legal framework more permissive of harm to the general public than is ordinarily allowed.

International human rights mechanisms provide specific guidance that is relevant for cyber security, and should be drawn on in the development of norms for responsible state behaviour in cyberspace. For example, reports of UN Special Procedures explain why strong encryption is necessary for the confidentiality of information and how network shutdowns are in violation of human rights law and unduly interfere with

the availability of information. There is a well established body of norms under international human rights law, namely the UN Guiding Principles on Business and Human Rights, which spell out the responsibility of the private sector to respect human rights, mitigate adverse effects, and remedy harm. This is a critical point, given that the private sector owns and/or operates most of the infrastructure, hardware and software upon which the internet relies.

3.3.4 Security for whom?

Perhaps the most pernicious threat, is that states exploit the serious nature of cyber security threats to take liberties to enable them to exert their power in cyberspace in ways that directly undermine human rights. When assessing a cyber security framework, it is essential to ask: security for whom? security from what? and security by what means? Too often the answers to these questions reveal that the state defines security as protecting itself from political instability, applies disproportionate measures to ensure its own preservation, and itself becomes the source of insecurity.

To give just a few examples, in Vietnam a cyber security law was passed last year that allows the government to force technology companies to hand over potentially vast amounts of data, including personal information, and to censor users' posts. The previous year in China, a cyber security law was adopted that requires companies to censor "prohibited" information, restricts online anonymity, including by requiring real name registration, and mandates the storage of Chinese users' data within the country. In Israel, the proposed Cyber Security and National Cyber Directorate Bill would give the government sweeping new powers to hack the computers or phones of any person or entity that is defined as a threat to cyber security and to access the device and extract data without a court order. Earlier this year, the Venezuelan government proposed the Constitutional Law of Cyberspace, which declares Venezuelan sovereignty over cyberspace and would require messaging service providers to censor content without a prior judicial order or respect for minimum guarantees for due process among other measures to extend state control of the internet.

Each of these examples demonstrates a government instrumentalising security at the expense of human rights, in particular the rights to privacy, freedom of expression, association and assembly, and incidentally, at the expense of cyber

security, i.e. the availability, confidentiality and integrity of information and its underlying infrastructure.

3.3.5 Putting cyber security on the rights track

In order to safeguard human rights in this digital age, it is time to start treating cyber security as a human rights issue.

First, there is the need to challenge the prevailing view that human rights are an impediment to security. Perhaps the most widely cited example of human rights standing in the way of security is the assertion that encryption, which is critical for exercising the right to privacy, impedes law enforcement in conducting its work. Time and again, governments make the case for building in backdoors and weakening encryption in order to provide access to encrypted communications for law enforcement. However, experts are in agreement that it is not possible to provide access to encrypted communications for one government without doing so for all government and for malicious non-state actors. To put it another way, weakening cyber security for law enforcement purposes cannot be done without weakening security for all, and putting everyone's human rights at risk. This is because cyber security is inexorably linked to human security, which is a fundamental human right. Cyber security and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security.

Second, it is critical to apply human rights-based approaches to cyber security laws, policies and practices. The danger of cyber insecurity should never be a used a pretext to violate human rights. Instead, recognising that individual and collective security is at the core of cyber security means that protection for human rights should be at the centre of cyber security policy development. At the international level, it is imperative to root deliberations on cyber security in international human rights law. The Freedom Online Coalition "Internet Free and Secure" working group developed a set of cyber security and human rights-focused policy recommendations towards ensuring that cyber security policies and practices are based upon and fully consistent with human rights – effectively, that cyber security policies and practices are rights-respecting by design. These recommendations, which have been endorsed by 30 FOC governments and over two dozen NGOs, are a useful starting point for rooting cyber security policies and practices in human rights.

Third, companies must respect human rights, and governments must hold them to account. The UN Guiding Principles on Business and Human Rights provide the necessary framework; however, there is a need for more scrutiny and oversight of technology companies – both of those that provide the hardware and software used for launching cyber attacks and those that serve as the first line of defence in cyber attacks. In addition to conducting human rights impact assessments to identify, understand, assess and address the adverse effects of their policies and practices on the enjoyment of human rights, they should be conducting cyber security due diligence to review the governance, processes and controls that are used to secure the information they process. Companies have advanced self-regulatory initiatives like Microsoft's Cyber security Tech Accord, which aims to respond to cyber security threats that put people's rights at risk, but does not take an explicit human rights framing, and therefore has some gaps.

Governments can also do more to regulate the technology industry to prevent and mitigate human rights violations as a result of cyber insecurity. For example, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recently called for a moratorium on surveillance technology. Such bold moves are needed not just for the surveillance technology industry, but for the technology sector writ large, to ensure that companies are not profiting off of human rights violations or treating people's data recklessly.

Fourth, cyber security processes need to be multistakeholder and inclusive, as well as multidisciplinary, infused with human rights and technical expertise. This means taking cyber security outside the confines of national security and intelligence agencies and challenging assumptions that cyber security is first and foremost a national security issue. Given that citizens are so often asked to make sacrifices in the name of national security, it is crucial that the bases for those sacrifices are scrutinised for their necessity and proportionality; that there is independent oversight of responses to national security threats to ensure that they are justified; and that there is more transparency as well as public debate to ensure that national security is not being equated with regime security.

Digital technologies present new and unforeseen challenges to human rights and security, which will require more documentation, research and analysis. Until cyber security and human rights are understood and treated as mutually reinforcing and complementary, both will suffer.[22]

[22]https://www.apc.org/en/news/why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

3.4DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)

The United States has unrivalled strategic tools, which it will use to develop superior military capability in cyberspace. The Pentagon has already started to look at how businesses can assist the government in combating the cyber threat. The chief executive officers and chief technical officers of information technology and defense firms now consult annually with senior officials from the Department of Homeland Security, the Office of the Director of National Intelligence, and the Department of Defense as part of the Enduring Security Framework, a public-private collaboration. The science and development agencies of the United States government have now turned their focus to cyber security. The National Cyber Range initiative, established by the Defense Advanced Research Projects Agency, is one of the most significant developments to emerge (DARPA). The Pentagon has had no such capabilities when it comes to cyberwarfare, despite the fact that the US military regularly drills units on target ranges and in a series of simulations.[23]This is why DARPA, which was instrumental in the development of the Internet decades ago, is creating the National Cyber Range, a virtual Internet that will enable the military to test its cyber defense capabilities before deploying them. Malicious applications intended to hack computer networks will also benefit from simulations. The National Laboratories of the Department of Energy have created machine farms that function as automated petri dishes, collecting live viruses from the Internet and monitoring their propagation. These diagnostic and teaching skills will help the US keep ahead of its adversaries' cutting-edge cyber weapons.

DARPA is conducting still more fundamental analysis that might boost the government's ability to attribute threats and blunt intruders' capabilities, reducing the offense-dominant nature of cyberspace. The military may update or retrofit computers, operating systems, and programming languages with cyber security in mind, according to the department, which is asking the scientific community to reconsider the fundamental configuration of the Pentagon's network infrastructure. Complex information technology systems would not improve immediately, but the United States has a good chance to engineer its way out of some of today's most troublesome vulnerabilities over the span of a century. The government must also improve its human resources. The Pentagon has expanded the number of cyber security experts on staff and improved their education. Which requires a rigorous credential program that now graduates three times as many data security experts each year as it did only a few years earlier.[24]

The Pentagon's network managers have been educated in "ethical hacking," which entails using adversarial tactics against the US's own networks in order to detect vulnerabilities before they are used by an attacker, in line with industry standards. And as the US government expands its cyber security workforce, it must

[23]APC, (2019) 'Why cyber security is a human rights issue, and it is time to start treating it like one', retrieved from: https://www.apc.org/en/news/ why-cyber security-human-rights-issue-and-it-time-start-treating-it-one

[24]Krotkov E, Blitch J. The Defense Advanced Research Projects Agency (DARPA) Tactical Mobile Robotics Program. The International Journal of Robotics Research. 1999;18(7):769-776. doi:10.1177/02783649922066457

acknowledge that long-term human resource dynamics are not encouraging. The United States accounts for just 4.5 percent of the global population, and several nations, including China and India, will train more highly skilled computer scientists in the next 20 years than the United States. If the US's cyber edge is based solely on amassing qualified cyber security experts, the US will lose the advantage.[25]
As a result, the US government must approach the cyber security problem in the same way it approaches other military challenges: with an emphasis on superior technology and competitiveness rather than statistics. To supplement the qualified cyber security experts in the US military, high-speed sensors, advanced analytics, and automated systems will be required, and such resources will be accessible only if the US commercial information technology sector remains the world leader, which will necessitate continued developments in research, technology, and education at all levels.

3.5THE THREAT ENVIRONMENT

About all the military does is made possible by information technology: logistics assistance, multinational command and forces, real-time intelligence, and remote operations. Each of these roles is largely reliant on the military's global networking backbone, which includes 15,000 networks and millions of computer machines spread across hundreds of countries' facilities. More than 90,000 employees work full-time to keep the system running. Digital technology in the military has progressed from an administrative instrument for increasing workplace production to a national strategic weapon in its own right in less than a decade. The United States' digital technology today gives it crucial advantages over any foe, but its dependence on information networks still allows adversaries to acquire useful intelligence about US capabilities and activities, obstruct conventional US armies, and threaten the US economy. The Pentagon is concentrating on a few aspects of the cyber challenge as it develops a strategy to fight these threats.[26]
First and foremost, cyberwarfare is asymmetrical. Because of the low cost of computation, US adversaries do not need to develop costly weapons like stealth fighters or aircraft carriers to pose a serious threat to US military capabilities. A dozen dedicated computer programmers will disrupt the United States' global logistics network, rob its operating plans, blind its intelligence capability, or obstruct its ability to deploy weapons on schedule if they discover a loophole to exploit. Because of this, many militaries are improving aggressive cyber capabilities, and over 100 international intelligence agencies are attempting to hack into American networks. Many countries have also shown their ability to undermine parts of the United States' information system.
The US barely gets it right when it comes to predicting when and when armed clashes will occur. It's also difficult to predict cyberattacks, particularly because both state and non-state actors are a threat. More importantly, since information

[25]Pippine J, Hackett D, Watson A. An overview of the Defense Advanced Research Projects Agency's Learning Locomotion program.The International Journal of Robotics Research. 2011;30(2):141-144. doi:10.1177/0278364910387681

[26]Feldstein, S. (2019) 'The Global Expansion of AI Surveillance,' Carnegie Endowment for International Peace, retrieved from: https:// carnegieendowment.org/2019/09/17/global-expansion-of-aisurveillance-pub-79847

technology is increasingly emerging, lawmakers have no historical experience to base their standards on. As a result, the US government must be realistic in its capacity to predict when and how this challenge will manifest; instead, it requires an approach that allows for organizational stability and adaptability.

3.6NEW STRATEGY

The Pentagon has officially accepted cyberspace as a modern area of warfare on a doctrinal level. Despite being a man-made world, cyberspace has become as essential to military operations as ground, sea, air, and space. As a result, the military must be capable of working inside it. The defense department needs an adequate operational framework to support cyberspace operations. The military's cyber security effort has been run by a loose confederation of joint task forces that are geographically and institutionally scattered for many years.[27] Defense Secretary Robert Gates ordered the restructuring of the task forces into a new four-star unit, the US Cyber Command, in June 2009, realizing that the scope of the initiative to defend cyberspace has outgrown the military's current systems. The US Cyber Command launched operations in May 2010 as part of the US Strategic Command. By October, Cyber Command should be fully operational.[28]

There are three missions for Cyber Command. First, it is in charge of the day-to-day security of all defense networks, as well as assisting military and counter-terrorism missions with cyberspace operations. Second, it establishes a transparent and accountable method for coordinating electronic warfare capabilities around the military. From the president of the United States through the secretary of defense, the commander of Strategic Command, the commander of Cyber Command, and on to individual military units around the globe, there is a single chain of command. Cyber Command manages commands within each branch of the military, including the Army Forces Cyber Command, the US Navy's Tenth Fleet, the 24th Air Force, and the Marine Corps Forces Cyberspace Command, to ensure that cyber security issues are a routine part of recruiting and equipping troops. Since military networks are not impenetrable to attack, ensuring that all tactical forces can operate in a degraded knowledge environment is an important part of the training mission.

The third mission of Cyber Command is to collaborate with a number of allies both within and outside the US government. Representatives from the FBI, the Department of Homeland Security, the Justice Department, and the Defense Information Systems Agency, as well as liaison officers from the intelligence community and allied nations, serve on-site at Cyber Command's Fort Meade headquarters. Cyber Command, in collaboration with the Department of Homeland Security, collaborates closely with private industry to exchange vulnerability intelligence and fix common vulnerabilities. Since information networks link a number of organizations, the United States' defense effort can only be effective if it is organized through the nation, with alliances, and with commercial partners. Given the offensive superiority in cyberspace, US defenses must be flexible. Since

[27]Freedom Online Coalition (FOC), (2015) 'Recommendations for Human Rights based approached to cyber security,' Working Group 1 "An Internet Free and Secure", retrieved from: https://www.freedomonlinecoalition.com/ wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final21Sept-2015.pdf

[28]Front Line Defenders, (no date) 'Security in A Box - Digital Security Tools and Tactics', retrieved from: https://securityinabox.org/en/

milliseconds matter, the US military must react to attacks when they occur, or even before they occur. To deal with this, the Pentagon has deployed a scheme that consists of three interconnected lines of protection, two of which are built on commercial best practices, such as maintaining up-to-date security technologies and firewalls, and sensors that track and map intrusions.

The third line of defense employs federal surveillance resources to provide highly advanced active defenses, and the government is applying all of these defenses in a manner that complies with its duty to defend Americans' civil liberties. The National Security Agency has pioneered programs that rapidly deploy protections to counter intrusions in real time, based on alerts issued by US intelligence capabilities. This active defense networks, which are part tracker, part sentry, and part sharpshooter, mark a significant change in the United States' approach to network defense.[29] They detect and avoid malicious code until it enters military networks by using scanning technologies at the gateway of military networks and the open Internet. Both security and intelligence networks in the ".mil" area are now protected by active defenses. Since certain intrusions will eventually elude detection and go undetected at the border, cyber protections in the United States must be able to track down intruders after they have gained access. This necessitates the need to search inside the military's own networks, and is part of the Pentagon's aggressive defense capabilities. Active security has been made possible by bringing the Department of Defense's joint cyber defense assets under one roof and connecting them to the signals intelligence required to predict intrusions and threats. One of the most significant reasons for the establishment of cyber command was to establish this connection. Because of the pace at which active defense systems must respond, network defense rules of engagement must be established in advance. It's not easy to come up with these protocols. Indeed, defining simple rules of engagement for reacting to cyberattacks has proven to be extremely challenging, and for good reason.

3.7 LET'S SUM UP

The overwhelming complexities of cyber security herald the dawn of a modern era of technology. The United States' greatest asset at this early stage is its understanding of the transition. The current situation reminds me of an urgent letter written to President Franklin D. Roosevelt on the cusp of a modern technical age. It was dated August 2, 1939, and it said, in part, "Certain facets of the current situation seem to necessitate vigilance and, if possible, prompt action on the part of the Administration. As a result, I feel it is my responsibility to put the following facts and suggestions to your notice." "Yours most sincerely, Albert Einstein," the letter read. Following Einstein's warning that breakthroughs in nuclear fission could lead to the creation of an atomic bomb, Roosevelt launched the Manhattan Project, which helped the United States prepare for the atomic age. While the cyber crisis does not have the same existential ramifications as the nuclear era, there are significant parallels. Potential adversaries will use cyberattacks to bypass overwhelming US advantages of traditional military strength in a way that is both instantaneous and difficult to track.

[29] Liaropoulos, A. (2015) 'A Human-Centric Approach to Cyber security: Securing the Human in the Era of Cyberphobia,' Journal of Information Warfare 14 (4), 15–24.

And if such attacks do not result in the same level of deaths as a nuclear attack, they have the potential to paralyze American society. In the long run, hackers' concerted hacking of American universities and companies could deprive the US of its intellectual property and competitive advantage in the global economy. These dangers are prompting the Pentagon to develop a new cyber security policy.
The strategy's main components are to provide an organizational structure for training, equipping, and commanding cyber defense forces; to use layered defenses with a strong core of active defenses; to use military capabilities to support other departments' efforts to secure the networks that run the US' critical infrastructure; and to build collective defenses with US allies. The aim of this policy is to make cyberspace stable so that revolutionary technologies will benefit both national security and economic security in the United States.

3.8FURTHER READING

- Press, 2008). 9 See "Country Profiles," OpenNet Initiative, Internet, https://opennet.net/country-profiles (date accessed: 30 October 2013).
- 2013). II Milton Mueller, Andreas Schmidt, and Bren- den Kuerbis, "Internet Security and Networked Governance in International Relations," International Studies Review 15 (2013), 86-104.
- RonaldDeibert, "Why NSA spying scares the world," 12 June 2013, CNN, Internet, http://www.cnn.com/2013/06/12/opinion/deibert-nsa-surveil-lance (date accessed: 30 October.

3.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How is DARPA contributing in cyber security?**

   DARPA is also working on more basic analysis that could help the government better attribute threats and blunt intruders' capabilities, rendering cyberspace a less offensive area. The military may update or retrofit computers, operating systems, and programming languages with cyber security in mind, according to the department, which is asking the scientific community to reconsider the fundamental configuration of the Pentagon's network infrastructure.

3.10 ACTIVITY

Explain the strategies adopted by Pentagon for cyber security. (1000-1500 words)

4

Unit 4: ROLE OF CIVIL SOCIETY

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Starting with first principles of security

4.4 Opening Up the Black Box

4.5 Shutting the Back Door

4.6 Let's sum up

4.7 Further reading

4.8 Check your progress: Possible Answers

4.9 Activity

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- the principles of security theory
- open government security programme
- shutting the back door for law enforcement and intelligence agencies

4.2 INTRODUCTION

As cyberspace has become the infra- structure for global communications, the security of the domain has become a top priority. Yet, rarely examined directly are the questions, security for whom and security for what? Although engineers like to think of cyber security as a technical problem requiring a “fix” or “patch,” security is always for someone and some purpose and is, therefore, always inherently political. In the absence of considered alternatives, the tendency has been to default to the Realist approach to statecraft and all that it entails. Not surprisingly, we are seeing reflexive policies that involve erecting defensive perimeters to the world outside; solutions that depend on hierarchy, secrecy, and classification; and defense and intelligence agencies taking on leading roles. These approaches result in the gradual erosion of checks and balances on power, self- reinforcing cycles of hostility and suspicions abroad, and a dangerously escalating arms race in cyber- space fuelled by a growing cyber security industrial complex.[30] In book, Black Code, the author has argued that in the headlong rush to security, liberal democratic countries are losing sight of that which they should be securing in the first place: a robust system of checks and balances that, supported by the free flow of information and commerce, cuts across domestic and international divides of like-minded countries and gradually results in the integration of security communities sharing a commitment to the rule of law and human rights. Part of the problem rests with the communities most dependent on the success of such a vision: global civil society.

Those who would consider themselves to be part of global civil society have been among the most persistent watch- dogs of governments and corporations, spotlighting violations of human rights online, and calling out surveillance and censorship. However, they have found it much easier to identify what they are against than what they are for, especially when it comes to securing cyber- space. Security is traditionally seen as an anathema to civil society, for some the language itself evocative of the very constituencies that need to be resisted. Yet, sidestepping the conversation will ensure only that citizens communicate in environments secured according to the interests and values of others. Civil society is moreover critically dependent on communications, and should see securing cyberspace as a top priority as much as any other stakeholder. To be sure, what is loosely called “global civil society” is hardly unified, and contains many divisions along ethnic, gendered, and regional lines. However, at a baseline, all of civil society depends on both an open

[30] Jensen, Michael &Danziger, J. &Venkatesh, Alladi. (2007). Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics. Inf. Soc.. 23. 39-50. 10.1080/01972240601057528.

and secure Internet, one not subject to disruption and through which ideas can be freely exchanged by citizens around the world. In the following article, the author lays out what he believes some of the core elements of that strategy should be, beginning with a consideration of first principles. Together these strategies are oriented around building a fortress for liberal democratic republics that can be extended as part of a global civil society strategy for cyberspace.[31]

4.3STARTING WITH FIRST PRINCIPLES OF SECURITY

The political nature of security begins with what is defined as the "object" of security, meaning that which is considered worth protecting. While the object of security in international affairs may seem too obvious to state, there is wide variation in objects of security, even in today's nation- state system. For some, the object of security is the entire country: its population, territory, and way of life. For others, it is more narrowly defined around the regime, party, or even an individual in power. It is remarkable how rarely such considerations of first principles around security are examined.[32] Part of the reason is that for so long, one tradition has had a monopoly on security discourse and practice. Once invoked, security tends to privilege Realist-associated institutional responses and elevate certain priorities in an almost instinctual fashion: hierarchy, secrecy, concentration of power, the erection of borders between "inside" and "outside," and the employment of military and intelligence agencies to positions of power and authority.

While these lessons have a long pedigree and were formed out of centuries of hard-fought experiences, they may not always be appropriate to the conditions of a time and place. There is also a lack of clearly articulated alternatives to this tradition, especially in civil society. Not surprisingly, those who consider themselves to be part of a global civil society, such as advocates of human rights, lack their own tradition of security from which to draw. Security tends to be seen by members of this community as some- thing to be resisted at best, or delegated to the men and women in uniform at worst. Those among civil society who are outraged today by revelations of government surveillance may even go further, believing that no government is good government. Yet, civil society is inherently dependent on the rule of law, without which human rights- including privacy, freedom of speech, and access to information-cannot be guaranteed. Without agencies capable of enforcing laws or defending against those whose aims are to destroy the very basis of liberal democracy, civil society networks would quickly find themselves extinguished. It is both undesirable and unrealistic to advocate doing away with government altogether.[33]

The question is not a matter of states versus no -states, but rather which type of state do we want? The work of Johns Hopkins, University Professor Daniel Deudney argues that there is a long- standing security theory at the heart of liberal democratic thought, one which is derived from the republican tradition of politics stretching to

[31]Cauce, A., and Srebnik, D. 1990. Returning to social support systems: A morphological analysis of social networks. American Journal of Community Psychology 18(4):609–616

[32]Davis, R. 1999. The web of politics: The Internet's impact on the American political system. New York: Oxford University Press

[33]Lessa, E. P. 1990. Multidimensional analysis of geographic genetic structure. Systematic Zoology 39(3):242–252.

ancient Greece. While having different elements, that tradition can be boiled down to core practices that mix and disperse authority around a system of checks and balances, in order to tie down and prevent the concentration of political power. Deudney has described these republican security practices as employing the structural principle of “negarchy,” namely, something in between the twin evils of anarchy and hierarchy. Republican security thinking is associated mostly with domestic political orders, but it is inherently an inter- national approach as reflected in the founding of the early United States of America and later the European Union, both of which sought to achieve a confederation of independent units but stopped short of full amalgamation into a consolidated state.

Republican systems of rule are designed to guard against not only internal hierarchy, but also external predation and empire. Reflecting on this theory in the con- text of cyberspace governance, it is noteworthy that the Internet exploded in a short period to become one of the most densely integrated of these transnational networks. However, the gradual encroachment of governments into Internet policy has imposed borders on cyberspace, perversely under- mining one of the pillars of republican security practice in the process. More than forty countries engage in some form of Internet censorship, including liberal democratic countries, with the censorship undertaken in secrecy using technologies developed by Western firms. Countering these tendencies requires a nuanced understanding of the interconnections between these multi-layered processes, and an orientation starting with first principles and working outwards. From this perspective, speaking about “Internet freedom” abroad while taking advantage of locally domiciled companies to subject communications to surveillance seems like self-serving hypocrisy. Instead, it is in the interest of liberal democratic governments to push for ever expanding transnational communications infrastructures that operate with the greatest degree of transparency and independence from specific jurisdictions, while working to strengthen and deepen practices of mixture, division, and restraint starting in the liberal democratic core and working outwards.

4.4OPENING UP THE BLACK BOX

At the heart of republican security practices is what Jeremy Bentham called a “system of distrust,” one in which elites are kept in line, in part, by fear of public exposure. Likewise, John Stuart Mill argued that exposure compels “deliberation and force[s] everyone to deter- mine, before he acts, what he shall say if called to account for his actions.” Government secrecy in a liberal democracy should be practiced infrequently with exceptional justifications, and closely monitored by independent oversight bodies. Over the years, however, and especially in response to the exigencies of 9/11, government secrecy has ballooned. Ironically, at the same time that elected officials have been campaigning on platforms of “open government,” security programs are being quietly buried in layers of classification and shielded from public scrutiny. For example, the deliberations of the U.S. court whose ostensive mission is to provide a check against the operations of the NSA, the Foreign Intelligence Services Court, are themselves shielded from public scrutiny.

At the same time, government agencies that operate with the most secrecy, notably signals intelligence, have mushroomed in scope and scale, their budgets and missions expanding. The influence of these pro- grams has extended into the private

sector, including scores of defence and intelligence contractors that service their programs, like Edward Snowden's former employer Booz Allen Hamilton. These companies are drawn into an orbit of classification and secrecy, some estimates as many as 1.4 million Americans hold Top Secret clearances. While a great deal of attention has focused on the adequacy of the United States system of checks and balances in the wake of the Snowden revelations, arguably its system of oversight is much more rigorous than those of other liberal democratic countries. In Canada, for example, the operations of the Communications Security Establishment of Canada (CSEC) - the Canadian counterpart to the American NSA are overseen by a single independent commissioner, a retired federal judge.[34]

There is no parliamentary oversight of the CSEC. Meanwhile, its budget and staff have grown considerably since 2001. Likewise, recent reports by the Guardian disclosed that officials in the U.K.'s Government Communications Headquarters (GCHQ) held the belief that "We have a light oversight regime compared with the US. Not only have these agencies ballooned in size, but some have also been given expanded responsibilities as lead agencies in cyber security. For example, the NSA and the U.S. Cyber Command share the same chief, General Keith Alexander. According to intelligence historian James Bamford, "never before has anyone in America's intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy." More important than Alexander's personal rule, however, is the gradual positioning of the NSA as the command agency for U.S. cyber security. While it certainly can make an argument for having the most advanced capabilities for the mission, the secrecy that surrounds the organization means that having it do so can further inter- national suspicion, undermine inter- national cooperation, and introduce military solutions to a domain that is primarily owned and operated by the private sector. A corrective to this excess should be an urgent priority, and a good place from which to start are the Tshwane Principles, drafted by 22 organizations and academic centers in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world. The principles recognize that withholding information from the public is often a necessary component to protect the full exercise of human rights.

4.5SHUTTING THE BACK DOOR

The prevailing paradigm of cyber security has brought about pressures on industry not only to provide governments with access to data they control, but also to build directly into their technologies access systems, known as "backdoors." Built-in backdoors for law enforcement and intelligence agencies are not new to the post 9/11 era. In a report published by the Center for Democracy and Technology in the United States in 2013, a group of twenty computer security researchers argued that "mandating wiretap capabilities in endpoints poses serious security risks," and that "building intercept functionality into products is unwise and would be ineffective, with serious consequences for the economic well-being and nation."[35]

[34]Muhlberger, P. 2004. Access, skill and motivation in online political discussion: Testing cyberrealism. Democracy online: The prospects for political renewal through the Internet, ed. P. M. Shane. New York: Routledge

[35]Shutting the Backdoor - Open Canada. https://opencanada.org/shutting-the-backdoor/

A republican cyber security policy will stress the opposite: promoting universal use of state-of-the-art cryptography, the introduction of protocols such as “https by default” and “two factor authentication,” and the implementation of open source applications to create trust across borders, rather than designing in those insecurities by nature. Regulations surrounding data deletion and policies like the “freedom to be lost,” which, although traditionally used in a rights-based context, have security ramifications insofar as they limit the amount of stored data that may be used for malicious purposes, are in accordance with this strategy. In a world of “Big Data,” in which so much of our information is routinely given away as part of our daily life, law enforcement and intelligence agencies need to find ways to work within this universe as it exists, rather than drill holes from the inside out in ways that undermine confidence and create additional risks for all of society.

4.6 LET’S SUM UP

These elements of a republican strategy for cyber security are only starting points. Most of them are hardly novel, and each in their own right have been widely and loudly advocated by many organizations and individuals. However, it is important to remind oneself occasionally that the whole is greater than the sum of its parts; tying each of these elements together (and no doubt others that the author has failed to include here) into a coherent strategy will provide support, coherence, and direction to what otherwise might be seen as isolated arguments. Civil society need not shy away from the cyber security debate. Indeed, there is a rich tradition of republican theorizing about security from which to draw that can help inform a robust alternative to the conventional Realist approaches dominating today. The recent NSA revelations offer an opening to make such an argument, and to push for practical solutions to widespread cyber security issues from a republican security point of view.

4.7FURTHER READING

- Ronald Deibert, “Why NSA spying scares the world,” 12 June 2013, CNN, Internet, http://www.cnn.com/2013/06/12/ opinion/ deibert-nsa-surveillance (date accessed: 30 October.
- Ronald Deibert and RafalRohozinski, Risking security: Policies and paradoxes of cyberspace security,” International Political Sociology 4» no 1 (2010): 15-32. 4 Barry Buzan, Ole Waever and Jaap de Wilde, “Security: A new framework for analysis,” London: Lynne Rienner Publishers, 1998.
- Daniel, Deudney, Bounding power: Republican security theory from the polis to the global village, (Princeton: Princeton University Press, 2008).

4.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How is existence of global societies relevant in present cyber security era?**

   Those who would consider themselves to be part of global civil society have been among the most persistent watch- dogs of governments and corporations, spotlighting violations of human rights online, and calling out surveillance and censorship.

4.9 ACTIVITY

Explain the reasons with incidents as to why global societies are concerned about cyber security. (1000-1500 words)

Block-2

CASE STUDIES / DATA PROTECTION

1

Unit 1: EQUIFAX DATA BREACH: CASE STUDY

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Background

1.4 Factors that contributed to the breach

1.5 External Responses to the Data Breach

1.6 Analysis of the Case

1.7 Equifax handling of the Incident

1.8 Problems Inherent with Credit Reporting Agencies

1.9 Government Response to the Incident

1.10 Let's sum up

1.11 Further reading

1.12 Check your progress: Possible Answers

1.13 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- factors contributing to the data breach
- Equifax data breach case
- government's response to the Equifax case

1.2 INTRODUCTION

One of the most notable cyberattacks of 2017 was the Equifax data leak. The attack has far-reaching consequences, involving millions of civilians as well as many corporations and government departments. In reality, the attack was so serious that the US Government Accountability Office was called in to review the incident and provide a report for Congress about how to deal with it. This chapter will investigate the facts and circumstances around this devastating cyberattack, as well as objectively examine the case's causes in order to draw conclusions on how to prevent similar exposures. Finally, a latest cyberattack would be discussed, as well as a measure of customer vulnerability to cybercrime vs. conventional crime.[36]

1.3BACKGROUND

Equifax is one of the top three credit reporting companies in the United States. Equifax announced on September 8, 2017, that it had been the target of a cyberattack that resulted in a major data leak. The world was stunned to find that 148 million US citizens' confidential personal details, including addresses, dates of birth, Social Security numbers, and driver's license numbers, had been hacked in this data breach. A total of 209,000 credit card numbers were also stolen, in addition to personal details. At the moment, the magnitude and extent of the Equifax data breach is unthinkable.[37]The vulnerability and criticality of the personal identification details in the financial information in this breach presented an issue whose size could barely be measured at the moment, despite the fact that prior breaches had been greater. The idea that Equifax's flagship offering is actually extracted from a database holding much of the US population's personal and financial records was one of the problems that compounded the Equifax data breach. Equifax keeps track of each individual's credit history, which includes personal identification details, identified addresses, and account numbers. Furthermore, since the data is collected by companies rather than people in the database, the system is not an opt-in system.[38] Lending institutions record information about payment history, balances, and other main information pieces while an individual borrows money. When anyone

[36]Thomas, Jason. (2019). A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach. 10.13140/RG.2.2.16468.76161.

[37]Marc Rotenberg, Testimony before the House Committee on Financial Services, Hearing on "Examining the Current Data Security and Breach Notification Regulatory Regime"

[38]Atleson, M. (2019, July 2019). Equifax data breach: beware of fake settlement sites. Retrieved from Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-beware-fakesettlement-websites

applies for a loan, the new lender examines this information in order to determine the borrower's credit value, which is then used to make a lending decision.[39]

1.4FACTORS THAT CONTRIBUTED TO THE BREACH

Equifax claimed in their original statement that criminals compromised their databases from May to July of 2017. A vulnerability known as Apache Struts CVE-2017-5638 allowed criminals to gain access to Equifax systems and cause the data breach. As users go to import files, this flaw takes advantage of exception handling problems in the software's Jakarta Multipart parser. This vulnerability allows attackers to execute arbitrary commands from a remote location using a constructed Content-Disposition, Content-Type, or Content-Length HTTP header with a Content-Type header containing the characters #cmd=string (NIST, 2018).[40] Apache Struts is a well-known platform for developing fast Java applications. Since this valuable product is used by many companies, it is an excellent target for numerous cyber criminals because it can provide an access point to a large range of victims and their data. The Apache Software Foundation identified the alleged flaw and released a patch to address it. Then they made an announcement to the rest of the planet to let them know about the problems. On March 7, 2017, the patch was issued. The Department of Homeland Security notified Equifax and other credit reporting agencies of the system's failure on March 8, 2017, and instructed them to apply the patch. The Apache Software Foundation contacted Equifax systems administrators on March 9, 2017, and instructed them to install the patch. Equifax completed a search of the infrastructure on March 15, 2017, eight days after the repair announcement, seven days after warning from the Department of Homeland Security, and six days after notification from the provider. The Apache Struts vulnerability was not found in the scanner study. As a result, until July 29, 2017, the networks were unpatched and vulnerable. Equifax's security department found malicious behavior on the network around this period. Equifax shut down the program for three days before enlisting the help of an outside cyber security specialist to launch a forensic review. Most archives have been compromised, according to the initial investigation. As a result, reports were made that the sensitive records of about 145 million Americans, 8,000 Canadians, and 693,000 British people had been hacked as a result of a data leak.

1.5EXTERNAL RESPONSES TO THE DATA BREACH

Equifax's lackluster reaction to the vulnerability warning and clumsy treatment of the intrusion notification drew widespread condemnation. Equifax wanted to develop a new domain and webpage to handle all of the information that needed to be disseminated as well as engage with impacted customers and stakeholders. This perhaps well-intentioned business maneuver highlights the difficulty of coping with the issue. Other parties quickly set up bogus settlement and information pages,

[39]Marc Rotenberg, Testimony before the Senate Banking Committee, Hearing on Consumer Data Security and the Credit Bureaus

[40]Deahl, D., & Carman, A. (2017, September 20). for weeks, Equifax customer service has been directing victims to a fake phishing site. Retrieved from the verge: https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishingidentity-monitoring

opening up new avenues for bribery and cybercrime, as well as more public confusion. The platform was also flagged as a phishing hazard, which added to the accident injury. Worse, Equifax customer support used their Twitter feed to point possible users to one of the illegal phishing sites. Customers were issued PINs with naming conventions depending on the date the accounts were frozen as they flocked to freeze their credit reports. Unfortunately, this rendered them convenient for cybercriminals to figure out and exploit, allowing for even more potentially destructive assaults.[41]

Equifax was also chastised for providing free credit monitoring when attempting to limit customers' right to sue them in the terms and conditions during the registration period. When the crisis worsened and spiraled out of control, policymakers at all levels began to note and launch investigations and interventions. Equifax eventually reached a $600 million settlement with the 50 state attorneys general in the United States. The federal government took care as well. The Federal Trade Commission investigated Equifax, and Congress held numerous hearings on the matter. Bills were passed in both the House and Senate covering credit reporting agencies' business practices and privacy.

1.6ANALYSIS OF THE CASE

This data breach exposed a number of serious flaws in Equifax's treatment of the incident, as well as concerns with credit reporting agencies and the incident response process. As a result, there are many takeaways from this landmark cybercrime. In the following parts of the chapter, we'll go through some of these lessons.

1.7EQUIFAX HANDLING OF THE INCIDENT

End-users are often cited as a primary target for cyberattacks, and technology professionals frequently advise proactive user training and awareness, as well as adult-oriented training methodologies, to avoid phishing attacks and identity theft. However, it seems that the most important causal factors in this situation were system maintenance procedures. The Equifax IT team, in particular, did not implement the patch when it was released. The IT department refused to apply the fix that would have eliminated the flaw after being prompted by several outlets such as the Department of Homeland Security and the tech provider.It's worth noting that Equifax's protection staff ran a check to determine whether the flaw was present in the framework.[42] The flaw was also not detected by the scan, according to reports. This raises the possibility of other IT machine management problems. One explanation is that the scanning program was not adequately patched or upgraded, and that its list of existing vulnerabilities did not include the necessary information to

[41]Frost, A. (2018, September 6). Equifax data breach: Still haven't frozen your credit since the huge hack? Here's how. Retrieved from USA Today: https://www.usatoday.com/story/money/2018/09/06/equifax-data-breach-how-freezeyour-credit-report/1136955002/

[42]Fruhlinger, J. (2019, October 14). Equifax data breach FAQ: what happened, who was affected, was the impact? Retrieved from CSO: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happenedwho-was-affected-what-was-the-impact.html

diagnose the vulnerability. Given that the flaw was well-known, another explanation is that the scanning program was unreliable or disabled.
However, in the author's view, it's more plausible that the scanning program was out of date and therefore unable to spot the flaw. It also suggests that the Equifax IT and compliance departments may have acted negligently. A search was run to see if the flaw was still there. On several occasions, detailed instructions for applying the patch were given. The fix was clearly not introduced. Why didn't the team just check the repositories for updates to make sure they were installed? In general, this is a simple procedure that would have automatically shown that the patch has not been implemented. Equifax has a fiduciary responsibility at the executive level, both ethically and legally, to warn concerned users that their details had been hacked and to try to rectify the situation. Equifax's treatment of the case, both before and after the incident, can only be defined as poor. As previously mentioned, the attack was primarily caused by Equifax's lack of patch management diligence and cluster reaction to instructions to apply a fix to correct a recognized weakness.[43] Following that, the company seemed to behave in a way that was inconsistent with efficiently disseminating facts about the attack or effectively addressing the issue. The corporation attempted to curb consumers' right to claim civil action and restitution by selling $1.8 million in company securities before the violation was publicly revealed, ostensibly to avoid losing money on these substantial amounts of stock shares. These activities seem to suggest that Equifax and its executive team members' reactions were motivated by possible financial motives. Executive benefits are sometimes cited as motivators for leaders to make decisions in their own best interests, rather than in the best interests of their clients or other stakeholders.[44]

1.8PROBLEMS INHERENT WITH CREDIT REPORTING AGENCIES

There were also threats at the time of the attack due to the intrinsic existence of the credit reporting agency structure in the United States. Consumers are unwitting participants in the systems; they did not and do not have the ability to opt out, and their knowledge is reported by the businesses in whom they do business. For the majority of customers in the United States, this poses an unapproved and often uninformed possibility. Following the attack, there was a lot of talk about how important it was to be able to freeze credit files. Credit records have gone from being able to be frozen for a small fee to being able to be frozen for free since then.

1.9GOVERNMENT RESPONSE TO THE INCIDENT

As previously said, the incident elicited responses from governments at all stages. The responses ranged from chastising Equifax to suing for damages to enacting stricter credit reporting agency and privacy laws, as well as strict penalties against

[43]Gressin, S. (2017, September 8). The Equifax data breach: what to do. Retrieved from The Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[44]Melin, A. (2017, September seven). Three Equifax Manager Sold Stock before Cyber Hack Revealed. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2017- 09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

Equifax. In addition to increased awareness and surveillance, the federal government spearheaded two concrete initiatives to resolve potential issues: improved credit report freezing and unfreezing capabilities, and a thorough examination of the need for data holders to alert users of data breaches. The passing of the Economic Growth, Regulatory Relief, and Consumer Protection Act is an example of this.[45]

1.10 LET'S SUM UP

The Equifax data breach was unprecedented at the time, and it was the worst and most complex data breach ever. The attack was triggered by a vendor-published identified vulnerability, and Equifax issued several alerts to install the fix that would mitigate the vulnerability. However, corporate systems maintenance and cyber security are extremely nuanced, and despite having a presumably massive IT branch, Equifax was unable to detect and trace the intrusion using traditional digital forensic techniques and systems administration procedures. Forensics investigations were carried out by an outside security firm. A catastrophic cybercrime with far-reaching consequences was enabled by the simple act of forgetting to download a patch and failing to search correctly to see if the patch was installed. New cybercrimes are created or perpetrated on a regular basis as a result of the evolving existence of technology and its growing use in everyday life and industry. When emerging technology is adopted, these crimes vary from the use of completely new tools to the commission of various forms of cybercrime, as well as the application of previous cybercrime methodologies to new goals. Cyber crime has become so common that more people are more concerned with identity fraud than about home burglaries. Cybercrime is becoming increasingly prevalent as a method of committing illegal acts due to its nuanced nature and economies of scale, as well as the lower expense and probability of committing the crimes. People are more vulnerable to cybercrime than conventional criminals because of the wide range of tools and touch points available.

1.11FURTHER READING

- Perez, L. (2017, September 8). 2019 Fed Meeting Predictions — A Fourth Fed Rate Cut Is Unlikely.
- Rajna, G. (2018). Equifax Data Breach. viXra. Retrieved 12 7, 2019
- The Apache Software Foundation. (2018). Apache Struts.
- Thomas, J. E. (2017). Lessons learned in management, marketing, sales, and finance incentive practices a decade after the Subprime Mortgage Crisis. International Journal of Business and Management, 12(3), 19-26.

[45]Oregon Department of Justice. (2019, July 22). 50 State Attorney Secure 600 Million from Equifax in the Largest Data Breach Settlement in History. Retrieved from Oregon Department of Justice: https://www.doj.state.or.us/media-home/news-media-releases/50- state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breachsettlement-in-history/

- Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business and Management, 13(6), 1-24.
- Thomas, J. E., &Hornsey, P. E. (2014). Adding Rigor to classroom assessment techniuqes for non-traditional adult programs: A liifecycle improvement approach. Journal of Instructional Research, 3, 27-37.
- Thomas, J., Galligher, R., Thomas, M., &Galligher, G. (2019). Enterprise Cyber security: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. Computer and Information Science, 12(3), 72-80.

1.12CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What vulnerability led to the breach at Equifax?**

   A vulnerability known as Apache Struts CVE-2017-5638 allowed criminals to gain access to Equifax systems and cause the data breach. As users go to import files, this flaw takes advantage of exception handling problems in the software's Jakarta Multipart parser. This vulnerability allows attackers to execute arbitrary commands from a remote location using a constructed Content-Disposition, Content-Type, or Content-Length HTTP header with a Content-Type header containing the characters #cmd=string (NIST, 2018).

1.13 ACTIVITY

Critically analyse the case study of Equifax substantiating your views with examples. (1000-1500 words)

Unit 2: WHAT'S UP WITH WHATSAPP? A TRANSATLANTIC VIEW ON PRIVACY AND MERGER ENFORCEMENT IN DIGITAL MARKETS

2

Unit Structure

2.1 Learning Objectives
2.2 Introduction
2.3 Privacy Law in the United States
2.4 Privacy Law in the European Union
2.5 Privacy and Digital Market Mergers
2.6 Facebook/Whatsapp Merger
2.7 Let's sum up
2.8 Further reading
2.9 Check your progress: Possible Answers
2.10 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Privacy laws of US and EU
- Privacy and digital market mergers
- Facebook/Whatsapp merger

2.2 INTRODUCTION

Data can be thought of as the knowledge economy's raw material, and companies in markets with customer-facing digital products and services have developed business models on the processing and use of consumer data. As companies in this industry combine, it will result in a significant increase in the reach and significance of customer data under a single company's jurisdiction. Some regulators and privacy activists are concerned that the merged entity's aggregated data, when exposed to more sophisticated "big data" analytic software, would produce particularly exposing portraits of customers, making data breaches more serious and raising the risk that data will be exploited in ways that will harm customers. The first line of protection in shielding users from the threats involved with combining vast amounts of data is privacy legislation.[46] Both the United States and the European Union have strong privacy laws that aim to increase transparency and customer protection of personal information. At the same time, as the storage and use of customer data becomes more common and predictive analytic software become more strong, some privacy regulators and activists on both sides of the Atlantic have called for antitrust oversight of the privacy implications of digital market mergers, a claim first heard nearly a decade ago in conjunction with Google's purchase of Double Click.
Recently, Facebook's decision to buy WhatsApp, a social messaging app, has reignited demands for antitrust solutions to address the privacy threats that may arise as a result of digital industry mergers. In this part, we'll look at how privacy and antitrust law work together to protect consumers from privacy threats posed by digital market mergers. Despite their different legal systems, the privacy regimes in the United States and the European Union share shared goals of fostering openness and market control, according to the report.In terms of antitrust, both jurisdictions have scrutinized mergers that could affect customer privacy solely on the basis of competitive consequences. Although this lens is broad enough to catch privacy threats associated with digital industry mergers that could build or boost market dominance, it isn't intended to capture risks that aren't related to a possible reduction in competition. Privacy threats that aren't linked to reduced competitiveness are better handled by enforcing privacy laws aggressively and incorporating the new safeguards needed to protect users into those regimes.

[46]1 See, e.g., Art. 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (Sept. 16, 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/ opinion-recommendation/files/2014/wp223_en.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC PRIVACY REPORT], available at http://www.ftc.gov/sites/default/files/documents/ reports/federal-trade-commission-report-protecting-consumer-privacy-erarapid-change-recommendations/120326privacyreport.pd

2.3PRIVACY LAW IN THE UNITED STATES

Despite varying regulatory mechanisms to defend privacy in the commercial sphere, privacy authorities in the United States and the European Union articulate common goals of open data policies, real customer preference, and "privacy by nature."The United States has a "sectoral" privacy regime, which requires businesses to follow a set of focused privacy laws covering categories of information that Congress has determined warrant special protection, such as children's online data under the Children's Online Privacy Protection Act, and health information held by medical providers, hospitals, pharmacies, and insurance companies under Non-public publicly identifiable information kept by financial institutions under the Gramm-Leach-Bliley Act, some information for decisions about a consumer's eligibility for credit, jobs, insurance, and other services under the Health Insurance Portability and Accountability Act (HIPAA), non-public personally identifying information retained by financial institutions under the Gramm-Leach-Bliley Act, certain information for decisions about a consumer's eligibility for credit, jobs, and insurance under the Gramm-Leach-BliUnder the Fair Credit Reporting Act (FCRA), or homes, and under the Video Privacy Protection Act, video rental documents.[47] The Fair Information Practice Principles, a series of privacy standards that has served as the framework for privacy regimes around the world, are the basis for these targeted regulations. As a result, any or more of the fair information practice rules, such as warning and an ability to respond to the storage and use of personal data, appropriate data access, and limitations on the reasons for which data can be collected, such as those contained in the FCRA, are usually mandated by U.S. privacy legislation. The key federal protections for the vast body of data that lies outside of these discrete areas are contained in the FTC Act's broad bans on "deceptive" or "unfair" commercial activities and practices. 8 After the 1990s, as the Internet became widely used, the FTC has used its power to regulate both online and offline commercial data activities. Data protection is a significant component of this regulatory operation.

The FTC has brought a relentless stream of lawsuits against corporations accused of failure to take appropriate action to protect customer data, enforcing the bans of both misleading and unfair practices. For example, in 2008, the FTC charged The TJX Companies with engaging in unreasonable and thereby discriminatory activities by storing and distributing personal information in its network in unencrypted code, failing to require network administrators to use strong passwords, and failing to use firewalls to restrict access among its customers, after what was at the time the largest breach of payment card details. Outside of data protection, the FTC has used the fraud ban to accuse businesses of making false or misleading statements about what customer data they would gather or how the data would be used or exchanged. For example, the FTC claimed in Snapchat that a smartphone app deceptively promised users that their videos and photo messages would be permanently deleted after a brief time period set by the user, while receivers had readily accessible means to save the videos and images. The FTC has challenged retroactive modifications to data procedures made without affirmative express approval, citing the ban on discriminatory actions or practices. The FTC, for example, said that when

[47]See, e.g., ASIA-PACIFIC ECONOMIC COOPERATION, PRIVACY FRAMEWORK (2005); ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (rev. ed. 2013)

Facebook revamped its website in December 2009, it unjustly overrode users' privacy settings, which had limited access to such information such as a profile picture and Friends List, without their informed consent. In addition, the FTC said that the misleading storage of extremely private data by the covert installation of spyware and key loggers on laptop computers was an unfair practice in lawsuits lodged against Aaron's rent-to-own franchisor, a number of its franchisees, and a software designer. In FTC v. Frostwire, LLC, the lawsuit claimed that a tech company's inability to warn consumers that many pre-existing files on computers and mobile devices would be reserved for public sharing was an illegal practice.[48]
Growing gaps in the United States' user protection legal system have arisen from changes in technology and corporate practices. Health data is now often in the possession of companies that are not protected by HIPAA, thanks to emerging technology and business models including smart workout bands and mobile health applications. Similarly, outside standard credit ratings, new products that claim to forecast or "rate" anything from the likelihood of a purchase resulting in theft to the feasibility of sending customers catalogs and the best rates to give consumers are typically exempt from the FCRA. To close these gaps, the FTC has backed "baseline" privacy regulations as well as data broker legislation. Similarly, the Obama administration has asked Congress to pass laws establishing a Consumer Protection Bill of Rights, which it hopes to enforce by multi-stakeholder meetings to develop cooperative codes of ethics in areas such as smartphone privacy disclosures and facial recognition.[49]

2.4PRIVACY LAW IN THE EUROPEAN UNION

Unlike the United States, where the Constitution only safeguards individual privacy from government action, the European Union has had a "protection of personal data" enshrined in the EU Charter of Fundamental Rights since 2000.[50] In addition, unlike the U.S. privacy regime, which is characterized by a complex mix of federal sectoral laws, the FTC Act, state laws, and private rights of action, a general EU data protection directive adopted in 1995 (General Directive) establishes comprehensive principles to limit the "processing"—a broadly defined term—of all "personal data," which includes "any information relating to an identifiable individual."Each member state enacts its own legislation to incorporate the General Directive, which is administered by one or more autonomous data protection agencies in each state. Personal data must only be processed for defined, explicit, and valid reasons under the General Directive, and must not be processed for an incompatible cause later. The approval of the user - the "data subject" in EU jargon - at the time of data

[48]See generally PAM DIXON & ROBERT GELLMAN, THE SCORING OF AMERICA: HOW SECRET CONSUMER SCORES THREATEN YOUR PRIVACY AND YOUR FUTURE 9–11 (2014), available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf; Press Release, Fed. Trade Comm'n, FTC Announces Agenda, Panelists for Alternative Scoring Seminar (Mar. 14, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-announces-agenda-panelistsalternative-scoring-seminar

[49]FTC PRIVACY REPORT, supra note 1, at 12–13; FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 49–54 (2014) [hereinafter FTC DATA BROKER REPORT]

[50]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) 31.

collection is one legal justification for collecting personal data. Furthermore, the storage and use of personal data must be equal to the reason for which it was collected in the first place. The General Directive also stipulates that data collection must be clear, which means that individuals must be informed of the intent of the processing as well as the recipients or groups of recipients to whom data is disclosed.[51] Similarly, data controllers must take reasonable steps to ensure the data's protection. Individuals have the freedom to view data gathered on them, according to the General Directive. In implementing the General Directive, the European Court of Justice recently held in Google Spain, SL v. González that search engines are "data controllers" and must delete connections to personal records that are incomplete, insufficient, unnecessary, or disproportionate in relation to the original reason for which the data is stored, upon request. The court clarified that the extent of this so-called "right to be overlooked" would be determined on a case-by-case basis and would have to be weighed against Internet users' rights to access content.

The EU is replacing the General Directive and member state implementation legislation with a single, statutory data protection policy across the EU in order to modernize its data protection regime. On March 12, 2014, the European Parliament adopted a draft of the new legislation. The establishment of a "one-stop shop" in which each data protection authority will manage all EU compliance activities for entities with EU headquarters in its jurisdiction is one of the main features of the Parliament-approved legislation. The law, which was passed by Parliament, would also provide a right to data portability, allowing individuals to move their data from one digital network to another. If a company is deemed to have breached the new law, it will face penalties of up to 5% of its annual revenue or 100 million euros, whichever is greater—a significant improvement from the actual fines already imposed on most individual data protection authorities. The final text of the legislation must be negotiated and approved unanimously by the EU Parliament and the EU Council of Ministers before it can become law.

2.5PRIVACY AND DIGITAL MARKET MERGERS

Despite increased attempts on both sides of the Atlantic to defend data privacy, privacy authorities and activists have turned to antitrust legislation to protect customers from the privacy threats associated with digital industry mergers. The combination of massive data sets that can result from mergers in this market, according to advocates and regulators, poses two key privacy threats. First, as businesses amass more detailed and revealing profiles of their customers, a single data breach will result in a broader trove of information falling into the hands of hackers, ultimately placing customers at greater risk of malicious behavior. Second, as richer data sets are subjected to predictive analytic tools, firms will be able to draw more revealing inferences about customers and make finer-grained distinctions between them, potentially increasing the likelihood of differential treatment in terms of what products and services are marketed to them, the prices they are charged, and the level of customer service they get, potentially outside of the

[51]See THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 35–39 (2012), available at http://www.white house.gov/sites/default/files/privacy-final.pdf.

telecommunications industry. In competition investigations, the European Data Protection Supervisor (EDPS), an EU privacy regulator, has emphasized the competitive ramifications of data, especially the relationship between data, entry barriers, and market influence.[52] The European Data Protection Supervisory Authority (EDPS) suggested in a preliminary opinion on the interplay between data protection and competition law that merger enforcement in digital markets should be based on a broader definition of consumer harm that goes beyond looking solely at competitive effects and accounts for risks to consumer privacy from the combination of large datasets that aren't always linked to a reduction in competition.

In the areas of data security, customer protection, and competition at the intersection of these areas, the EDPS called for further consultation among regulators. Many of these topics were revisited in a follow-up workshop and study. 37 In her opposition from the FTC's decision to close its inquiry into Google's purchase of DoubleClick in 2007, then-FTC Commissioner Pamela Jones Harbour raised some of the questions that the EDPS raised. Harbour has pressed enforcers to create a more sophisticated methodological system for assessing the antitrust ramifications of privacy and big data since leaving the department. Howard Shelanski, then-FTC Bureau of Economics Director, has also recommended that antitrust enforcers focus on the potential exclusionary effects of acquiring customer data, which "can reveal horizontal dimensions of facially vertical conduct and transactions," and recognize privacy protection as a significant non-price dimension of competition in digital markets, in a letter written in his personal capacity, Revisiting Google/DoubleClick. In 2007, after investigating Google's acquisition of DoubleClick, the FTC for the first time publicly grappled with the intersection of privacy and antitrust. In both the United States and Europe, Google was the leading source of search advertisements, and both firms were major players in the market for online display advertising, which consists of graphic advertisements that appear on websites that use icons such as corporate logos to create brand identity. Websites also offer premium advertising space, which is typically found in the top half of a website, to in-house personnel and rely entirely on third-party "ad servers" to handle the scheduling and location of those advertisements.

Websites typically use "ad intermediaries" to monetize their less lucrative real estate, which buy, aggregate, and market the property to marketers. Google was a major online advertisement intermediary for its AdSense product, and DoubleClick was a leading online ad server. The proposed consolidation of data held by Google and DoubleClick on user web search and browsing behavior sparked concerns among privacy advocates. The Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD), and the United States Public Interest Research Group (US PIRG) filed a lawsuit with the Federal Trade Commission (FTC) opposing the merger on the basis of privacy concerns. They also believed that combining the data would give Google a strategic edge over competitors in both search and display ads, enabling it to "monitor the process of monetizing web content." The FTC and the EC also published a thorough review of the transaction's strategic consequences as part of their unconditional approval of the merger.

[52]Robert McMillan, You May Not Use WhatsApp But the Rest of the World Sure Does, WIRED (Feb. 20, 2014, 8:17 PM), http://www.wired.com/ 2014/02/whatsapp-rules-rest-world/; Mike Isaac, Zuckerberg: More Than 200 Million People Use Facebook Messenger, RE/CODE (Apr. 23, 2014, 3:04 PM), http://recode.net/2014/04/23/zuckerberg-more-than-200-millionpeople-use-facebook-messenger.

In the competition for web advertisements or utilities, both companies determined that Google and DoubleClick were not near real or future rivals.[53] They also discovered that, due to its lack of market control, DoubleClick could not remove content intermediation competitors by bundling AdSense with DoubleClick's publisher ad server. Since DoubleClick's contracts did not allow Google to use the details to target advertising, and Google committed that it would not combine the data post-merger, no jurisdiction was convinced that the combining of data would offer AdSense an anticompetitive advantage over rivals.More specifically, both jurisdictions determined that, even though Google amended or broke these arrangements, DoubleClick's data were not exclusive, and that rival ad intermediaries could obtain comparable data of similar quality and quantity from other outlets. The FTC determined that the antitrust laws did not include a reason to attempt to prohibit or enforce restrictions on a merger solely to protect privacy, despite voicing a firm commitment to privacy and acknowledging that FTC workers have recently proposed a package of privacy standards for online behavioral advertisements. The FTC has stated that privacy is a non-price dimension of competition, and that it has the right to intervene where a deal is likely to minimize competition on that basis. However, it concluded that harm to competition on the basis of privacy was no more possible in this deal than harm to competition on the basis of price or other non-price dimensions. As a result, it came to the conclusion that "privacy interests, as such, do not provide a basis for challenging this transaction."The EC also assessed the agreement purely on the basis of its competitive consequences, while stressing that its decision did not affect the parties' different obligations under European data protection legislation.

2.6FACEBOOK/WHATSAPP MERGER

Related allegations were made to the FTC during its latest investigation of Facebook's planned purchase of WhatsApp.[54] Facebook, a social network with over a billion active monthly users worldwide, now provides networking platforms that enable users to send and receive text messages, images, and other digital content through its "Messenger" mobile app and its social network's messaging feature. Facebook revealed on February 19, 2014 that it had decided to pay $16 billion for WhatsApp, an instant messaging service. WhatsApp, like Facebook Messenger, has a smartphone app that helps members to deliver text messages and other multimedia content to other WhatsApp users over the Internet without having to pay for short message service. WhatsApp had 450 million subscribers globally when the acquisition was completed, with the bulk of them based outside of the United States. Messenger has 200 million daily users, according to Facebook. WhatsApp has marketed itself, at least in part, on the fact that it would not mine users' personal data to sell ads. "Your data isn't even in the picture," WhatsApp claims. We simply don't care for all of it." 50 WhatsApp advised users on the day of the takeover that the deal would change "nothing" for them in this respect. A few days later, Facebook CEO

[53]See Ellen Nakashima, Privacy Group Objects to DoubleClick Deal, WASH. POST (Apr. 20, 2007), http://www.washingtonpost.com/wp-dyn/content/ article/2007/04/19/AR2007041902647_pf.html.
[54]Complaint at 7–9, Facebook, Inc., FTC Docket No. C-4635 (July 27, 2012), available at http://www.ftc.gov/sites/default/files/documents/cases/ 2012/08/120810facebookcmpt.pdf

Mark Zuckerberg was quoted as saying that the company would not “change its plans about WhatsApp and how it uses user data.”
Despite these promises, privacy activists expressed reservations about the deal. EPIC and CDD filed FTC lawsuits opposing the planned purchase, repeating many of the claims leveled against Google/DoubleClick. They argued, in particular, that Facebook’s business model contradicted WhatsApp’s assurances to subscribers regarding how their mobile data would be gathered and used, and that WhatsApp failed to properly reveal that its privacy obligations could be rescinded or that customer data could be moved in the case of an acquisition.They asked the FTC to look at WhatsApp’s actions and use its “authority to review mergers” to put a stop to Facebook’s planned takeover of WhatsApp before the questions raised in the lawsuit is addressed. The groups asked the FTC to “order Facebook to insulate WhatsApp users’ details from links to Facebook’s data collection practices” if the transaction was approved. The FTC cleared the transaction on April 10, 2014, according to Facebook. The FTC does not usually release a statement outlining the specifics of its analysis when it concludes a merger investigation without taking action, and it did not do so here. However, on the same day as Facebook received approval, Jessica Rich, Director of the Federal Trade Commission’s Bureau of Consumer Protection, wrote to Facebook and WhatsApp, stating that Facebook’s acquisition of WhatsApp would not invalidate the commitments provided by both companies in WhatsApp’s privacy policy, as well as public comments made by both companies regarding privacy when the deal was revealed.
As a result, Rich clarified, businesses can not make any material changes about how they employ data already gathered from WhatsApp users without affirmative express permission, nor can they misinterpret how they keep WhatsApp consumer data. Failure to take these measures, she warned, may be considered misleading or discriminatory actions and activities, in breach of the FTC Act and a 2012 FTC consent order against Facebook. Rich’s note, although released at the conclusion of the inquiry, did not place restrictions on the merger, as the FTC does when it has cause to suspect an agreement would damage competition in the consent decree process.[55] Instead, the letter spells out the responsibilities that all businesses must meet when it comes to the acquisition, handling, and utilization of customer data, both before and after a merger. On August 29, 2014, the EC launched an investigation into the Facebook/WhatsApp merger. On October 3, 2014, the European Commission announced that the deal had been approved without conditions, stating that the merger was unlikely to affect competition in three areas of concern: consumer information services, social networking services, and online advertisement services. In terms of networking services, the EC determined that, while Facebook Messenger and WhatsApp serve identical roles, the companies are not direct competitors, owing to the fact that Messenger links users via their Facebook accounts, while WhatsApp relies on cell phone numbers.
Consumers use the services in a variety of ways, according to the EC, with those using both apps on the same computer. Furthermore, the European Commission determined that the demand for digital connectivity platforms was quickly expanding and that the obstacles to introducing new applications were limited. Although the EC acknowledged that network effects can often limit entry in telecom markets, it

[55]U.S. Horizontal Merger Guidelines, supra note 64, at 2; Guidelines on the Assessment of Horizontal Mergers Under the Council Regulation on the Control of Concentrations Between Undertakings 2004 O.J. (C 31) 5, ¶ 8, available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX: 52004XC0205(02).

determined that the merger would not lift hurdles because “consumers can and do use multiple applications at the same time and can quickly migrate from one to another.”Similarly, the European Commission concluded that in the field of social networking, the companies are at most “distant rivals” in a competitive industry with no clear borders and a large number of potential participants. Finally, the European Commission dismissed the possibility of competitive damage in online advertisements. The EC determined that even if Facebook used WhatsApp to extend the store of data it uses to target ads, it would also face significant rivalry in this area, in part because data on users’ online activity is open to competitors from alternative outlets, as it did in Google/ DoubleClick. The EC did not analyze privacy concerns associated with the “potential data concentration” that were not applicable to evaluating competitive results when it approved the merger. Instead, it argued, as it had in the case of Google/DoubleClick, that “any privacy-related issues arising from the enhanced accumulation of data under Facebook’s jurisdiction as a result of the purchase do not come within the limits of EU Competition law.”

2.7 LET’S SUM UP

Despite the possible connection between privacy issues and big data mergers, guidelines from both the US and the EU clearly signals that no jurisdiction can use antitrust regulation to oppose a deal that poses privacy concerns without causing a reduction in competition. In both Google/DoubleClick and Facebook/WhatsApp, the FTC and the EC rejected the opportunity, and a different conclusion would be inconsistent with both jurisdictions’ takeover compliance rules, which examine transactions exclusively on the basis of competitive results.As a result, merger enforcement has the power to supplement privacy legislation only in such situations where protecting competition still protects consumer privacy. Antitrust authorities in the United States and the European Union have yet to respond in a situation where the link was obvious. However, as emerging technology and business models make data collection and processing a virtually universal part of daily life, we should anticipate concerns about antitrust enforcement’s position in shielding customers from privacy threats associated with digital sector mergers to begin to appear in transaction reviews on both sides of the Atlantic.

2.8FURTHER READING

- The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 35–39 (2012).
- Joseph E. Stiglitz, Imperfect Information in the Product Market, in 1 Handbook of Industrial Organization.

2.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What privacy policy and principles are followed by United States?**

The United States has a “sectoral” privacy regime, which requires businesses to follow a set of focused privacy laws covering categories of information that Congress has determined warrant special protection, such as children’s online data under the Children’s Online Privacy Protection Act, and health information held by medical providers, hospitals, pharmacies, and insurance companies or Non-public publicly identifiable information kept by financial institutions under the Gramm-Leach-Bliley Act, some information for decisions about a consumer’s eligibility for credit, jobs, insurance, and other services under the Health Insurance Portability and Accountability Act (HIPAA), non-public personally identifying information retained by financial institutions under the Gramm-Leach-Bliley Act, certain information for decisions about a consumer’s eligibility for credit, jobs, and insurance under the Gramm-Leach-Bli or Under the Fair Credit Reporting Act (FCRA), or homes, and under the Video Privacy Protection Act, video rental documents. The Fair Information Practice Principles, a series of privacy standards that has served as the framework for privacy regimes around the world, are the basis for these targeted regulations.

2.10 ACTIVITY

Critically analyse the privacy laws of United States and European Union. (1000-1500 words)

3

Unit 3: FACEBOOK DATA THEFT IN INDONESIA

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Problems and Methods

3.4 Data Breaker Facebook in Indonesia: Case Analysis

3.5 Expert Opinion Regarding Facebook data breaker case

3.6 NGO Comments on the Hack top of Privacy

3.7 The Government Measures

3.8 Let's sum up

3.9 Further reading

3.10 Check your progress: Possible Answers

3.11 Activity

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Overview of crimes affecting economy
- Different kinds of cybercrimes using the computer and Internet
- Legal provisions pertaining to it

3.2 INTRODUCTION

The use of information technology in Indonesia has increased positively from year after year. Progress has been mentioned since the entry of the internet theology to the homeland since in 1988. The harmony between the development of information technology with the media and telecommunications today has resulted in a growing variety of services and existing products. The convergence of these technologies is called telematics (telecommunications, media, and informatics). The use of the Internet in various fields in our lives not only makes things easier but also causes some problems, one of which is the legal problem. One of the legal issues which may occur are issues related to the protection of privacy rights. The right to privacy is the privacy rights possessed by a person of his or her privacy. This right becomes private because it involves information that cannot be owned or submitted to all party without the permission of the owner of that identity. Some experts express this basic understanding of the right to privacy.[56]

Professor of public administration law from the University of Colombia, Alan Westin, defines the right to privacy as claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. The extent of privacy coverage usually makes the number of privacy settings in a country, both in type and level.[57] The notion and scope of other privacy concepts often referred to be the formulations developed by William Posser, referring to at least four things: (a) Disturbance of a person's act of alienation or aloofness, or interference with his relationships (b) Disclosure of personal facts publicly embarrassing (c) The publicity that puts a person wrong in public opinion (d) Unauthorized control of a person's likeness for the benefit of others.3 In international legal instruments, freedom of privacy is recognized as inherent basic rights to every human being. This provision is contained in the Universal Declaration of Human Rights. The Declaration has provided the legal basis for its member states in respect of the state's obligation to protect and respect the right of the individual's private citizens.

This provision is explicitly stated in Article 3 and Article 17 of the Universal Declaration of Human Rights. Article 3 set the right of the person as follows: "Everyone has the right to life, freedom, and liberty as an individual. "While Article 17 to protect the freedom in two paragraphs, namely: (1) Everyone has the right to own property alone or jointly with others; (2) No one shall be deprived of his property arbitrarily. Both the terms of the Universal Declaration of Human Rights above

[56]AF Westin, Privacy and Freedom, New York: Atheneum, (1967), pp. 7-8

[57]Natamiharja, Rudi. (2018). A Case Study on Facebook Data Theft in Indonesia.FIAT JUSTISIA. 12. 206. 10.25041/fiatjustisia.v12no3.1312.

provide for the broad protection of the right to privacy. But this is the embryo of the emergence of more specific protection classified into two classes of protection, first against civil rights and political rights, the second is the protection of economic, social and cultural rights or known as "ECOSOC" originating from International Covenant on Economic, Social and Culture Rights. Furthermore, the International Covenant on Civil and Political Rights (ICCPR), which was born on December 16, 1966, through Resolution 2200A and entered into force on 23 March 1976 provides more protection for the rights of the human person. Indonesia has ratified the ICCPR on 28 October 2005 through the Law of the Republic of Indonesia Number 12 the Year 2005 on the Ratification of the International Covenant on Civil and Political Rights.

The State of Indonesia state based on the rule of law and it's obliged to embody this international provision in a positive, applicable and positive contribution to its citizens. The importance of this rule must be felt in everyday life.[58] So that the people of Indonesia do not feel anxious personal data will be used or known to other parties that he does not desire. One example of cases of personal data protection in Indonesia is about the theft of users of social media data Facebook. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million users of Facebook, about 1 million of whom belong to users of Facebook in Indonesia. Indonesia is the third biggest country after the United States and the Philippines whose data are used. This data theft incident stems from the cooperation of Facebook and the application "thisisyourdigitallife." According to data compiled by Facebook Indonesia, 748 people have installed the application "thisisyourdigitallife" from November 2013 until December 2015. There are additional more than 1 million users who are affected by the friends of the user application. Then there are a total of 1,095,918 users whose data are stolen or 1.26 % of the total affected users globally. The meeting between the Commission 1 of the House of Representatives and Facebook been held. House of Representatives worried about Facebook data will affect the Indonesian political year of elections and elections simultaneously 2019 because Cambridge Analytica reportedly ever used a Facebook user information related to US presidential elections in 2017 and where the underdog Trump has managed to win his fight with Hillary Clinton. The disappointment of the House against Facebook is the absence of law enforcement from Facebook to third parties (Cambridge Analytica). The government's irresponsiveness in taking action has sparked the question of whether the provision in Indonesia is sufficient to cover its citizens or whether it is the House of Representatives' reluctance to resolve the issue. After the amendment of the The 1945 Constitution of the Republic of Indonesia (Undang-UndangRepublik Indonesia 1945), Law Number 11 on 2008 of Information and Electronic Transactions or abbreviated as the ITE Law was established. Then some articles of the law have improved in 2016 which became known as the Law Number 19 Year 2016 on the Amendment of Law Number 11 on 2008 of ITE. The establishment of the ITE Law is a mandate of the 1945 Constitution of the Republic of Indonesia, including articles relating to personal data, rights to privacy. In the elucidation of Article 26 paragraph 1 of Law Number 19 Year 2016 it is stated that the definition of personal rights is, the right to enjoy private and free life,

[58]Oik Yusuf, "Data 1 JutaPengguna Facebook Indonesia Dicuri", Kompas, April 05, 2018, https://tekno.kompas.com/read/2018/04/05/10133697/data-1-juta-user-facebook-indonesiadicuri, (accessed June 12, 2018).

the right to be able to communicate with others without spying action, the right to monitor access to information about personal life and data someone.
In Article 17 paragraph 3 of Regulation of the Minister of Communication and Informatics Number 12 of 2016, it is clearly stated that the Telecommunication Service Provider must keep the data and the identity of the customer confidential. The rules of personal data protection are outlined in the Ministerial Regulation No. 20 of 2016 on Personal Data Protection (PDP) set on November 7, 2016, enacted and effective from 1 December 2016. In the rule, it is stated that Personal Data is certain personal data stored, cared for, and safeguarded by the truth and protected by its secrecy. In this rule, an electronic system that can be used in the process of protecting personal data is an electronic system that has been certified and has internal rules on the protection of personal data which must pay attention to aspects of the application of technology, human resources, methods, and costs. The owner of the personal data, is entitled to the confidentiality of his data; have the right to lodge a complaint in order to settle a private data clause; entitled to access to obtain historical personal data; and has the right to request the destruction of certain personal data belonging to him in the electronic system. Through the existing personal data rules in Indonesia, it can be concluded that the protection of personal data in Indonesia is insufficient because it has no comprehensive laws or rules regarding the protection of personal data protecting its citizens from data misuse. It is, therefore, necessary to create a Personal Data Protection Law that has clarity of rules on the recovery of victims. Citizens also need to be educated about digital privacy to understand the potential risks that exist and the right to protect privacy and personal data.[59]

3.3PROBLEMS AND METHODS

Based on the background described above, the first issue to be described in this chapter is the extent to which regulations in Indonesia have covered the protection of personal data. The second issue, what the Government of Indonesia should take policies and steps in providing privacy data protection?

3.4DATA BREAKER FACEBOOK IN INDONESIA: CASE ANALYSIS

In 2013, Cambridge University researchers named AleksandrKogan created a personality quiz app, “thisisyourdigitallife.” Mark Zuckerberg revealed that the Kogan app is in use by around 300,000 people all of whom are willing to share their data as well as some data from their friends. Then Facebook changed the platform policy to limit the data accessible to the app a year later.[60] Such changes make developers like Kogan unable to request friend data from users unless their friends also access the app. In 2015, Facebook got information from the media that Kogan has shared

[59]A sample case can be found at https://tekno.tempo.co/read/1080112/dpr-bert -facebookbesok-bahas-skandal-data.
[60]KustinAyuwuragil, “KronologiPembobolan Facebook oleh Cambridge Analytica”, CNN Indonesia, March 03, 2018, https://www.cnnindonesia.com/teknologi/20180322194919-185- 285163/kronologi-pembobol-facebook-oleh-cambridge-analytica.

its data on Cambridge Analytica. Kogan has violated Facebook's policies for illegally obtaining data so that the platform removes the Kogan app. Cambridge Analytica does not delete all data as they promised before. Facebook took action to block Cambridge Analytica from its services. Cambridge Analytica argues that they have deleted all the data. They even agreed to be audited forensically by the Facebook-appointed company, Stroz Friedberg, to confirm the incident. The misuse of data by Kogan is widely cited as the largest data theft in history. Facebook reveals the number of users whose data is utilized by Cambridge Analytica to reach 87 million Facebook users, about 1 million of whom are owned by Facebook users in Indonesia. Indonesia is the third largest country after the United States and the Philippines whose data is utilized without seizing Facebook users.[61]

3.5EXPERT OPINION REGARDING FACEBOOK DATA BREAKER CASE

Cyber security expert, PradamaPersadha expertise from Indonesian Security Research Institute of Cyber and Communications assesses that Indonesia is difficult to act firmly against Facebook in case of data leakage involving data of more than one million users of social media applications owned by Indonesian citizens. This is because Indonesia does not have high bargaining power. Facebook Indonesia is currently still searching for data related to the leak and promised to conduct an internal audit as soon as the data is obtained even without detailing when the investigation was completed.[62] This promise has previously been conveyed by representatives of Facebook Indonesia in a Public Hearing Meeting (RDPU) with the Commission 1 House of Representatives, in April. Commission 1 of the House gives a one-month deadline for Facebook to submit its internal audit results. The results will be used to measure potential hazards that could result from data leak incidents. Meanwhile, he said that the call to Facebook manager in Indonesia would not have a significant impact on the settlement and follow up of the case. Because currently, Indonesia does not have "bargaining power" to force Facebook to follow government rules. On the contrary, according to Pratama, this case should be momentum for Indonesia to start its independence in the field of social media application services, while exemplifying China that prohibits Google to operate in the country and has its microblogging site called Weibo. But he admitted it is still far to materialize considering Indonesia has no resources either Human Resources (HR) and infrastructure. For now, the least that the government can do is to urge the FB to minimize the impact of data leakage for example if it is used for political purposes such as in the United States.

3.6NGO COMMENTS ON THE HACK TOP OF PRIVACY

SintaDewi, Chairman of Cyber Law Center in Faculty of Law Padjadjaran University, stated that the interests of personal data protection regulations are increasing. This will be related to information technology business on security and data protection. It

[61]Fatimah KartiniBohang, "DPR BeriWaktu Facebook 1 Bulan", Kompas, April 17, 2018, https://tekno.kompas.com/read/2018/04/17/16240047/dpr-beri-waktu-facebook-1-month

[62]Antara, "Data Bocor, Elsam: Menutup Facebook BukanSolusi" Tempo, April 11, 2018, https://bisnis.tempo.co/read/1078332/data-bocor-elsam-closing-facebook-not-solution.

also becomes one of the necessities in ensuring the sustainability of the digital economy in the future. Deputy Director of Research ElsamWahyudiDjafar, strengthen SintaDewi's opinion citing the resolution of the board of Human Rights in 2012 and 2013 adopted by the UN General Assembly which refers to Article 19 of the Covenant on Civil Rights and Political, states that: "the protection of all people when they are offline it will also apply when they are online "and" privacy protection on someone when they are offline it is also attached if they are online ".[63] Under both resolutions, the UN encourages member states to revise its privacy-related national laws. Facebook's case according to WahyudiDjafar, is an analytic data engineering that is not in line with the protection of the privacy of its citizens. If it persists, this practice will be perpetuated by affecting the preferences of the social choice of the social user with the consequences of excluding the rights of individual citizens. Hearing the explanation of experts from the civil society Vice Chairman of Commission I of the House of Representatives, Satya WidyaYudha acknowledges the urgency of this PDP Act. Even He also urged the Parliament to make laws for the PDP as a law a priority in the 2018-2019 national legislation. According to him, at this hearing, there was not a single fraction against the establishment of the PDP Law, so there is no reason for the House to postpone it. The Institute for Policy Research and Advocacy (Elsam) believes that closing Facebook access in Indonesia due to the misuse of user data by third parties is not the right solution.

Deputy Director of Research ElsamWahyudiDjafar encourages the implementation of audits with the government and Facebook to find out where the violations, what data is leaked, and what data is transferred. The issue of blocking or closing is according to him, usually depart from content issues, but for Facebook started from the issue of personal data of Facebook users. So do not have the right reasons if there is a Facebook shut down. When Facebook is closed, he fears it will limit the right of public information that has been able to communicate through Facebook and retrieve information from social media. In addition to a joint audit, it proposes a recovery mechanism against Facebook users who violated their privacy, then the obligations that must be charged to Facebook, such as updating terms of service or privacy policy to comply with privacy provisions. This is done so that the practices of alienation or misuse of data do not happen again. Also, in the future, Facebook needs to be encouraged to educate its service users, not only do recording of data or content uploaded on Facebook for large-scale data collection. In response to this Facebook case, Elsam sees the importance of placing human rights as the direction of its development. Human rights must be formulated in the form of a legal instrument as a guarantee of public protection. Normative forms are important for placing state responsibility and affirming the role of corporations in protecting people's privacy rights. This assurance of protection will ensure that technology and machinery work including artificial intelligence, for the benefit of data collection, will be in line with the principles of privacy protection. It can be concluded that the government has done various actions to solve the case of personal data protection data theft Protection of this Facebook, but the action is not sufficient because until now there has been no settlement from the Government and Facebook. The law in Indonesia implicitly provides for the guarantee of the right to privacy. Unfortunately, the legal regulation has not been properly outlined in the level of legislation.

[63]Quoted from http://elsam.or.id/2018/05/elsam-menghadiri-rapat-dengar-pendapat-umumdari-panja-pengamanan-data-ponsel-komisi-i-dpr-ri/.

Countries with low data protection laws such as Indonesia may be subjected to irresponsible companies for theft of personal data for their benefit.

3.7THE GOVERNMENT MEASURES

Minister of Communications and Informatics, Rudiantara, said his side keeps escorting the effort to hold Facebook accountable. Because of the possibility of account data in Indonesia abused that is to affect the results of elections next year (2019). The government has sent a letter to Facebook related to the theft of Facebook data in Indonesia to request confirmation and explanation of the case.[64] The government can also press Facebook to immediately close access to applications that allow the theft of personal data users. The company should not submit to the account owner to actively disable the leak-prone application. Facebook needs to be responsible for the privacy of its users. The Ministry of Communication and Informatics does not stand alone but also cooperates with the police. The Ministry of Communication and Informatics only takes care of administrative sanctions, while for criminal sanctions the process is carried out by the police. Relate leaked data social media platform Facebook, Rudiantara rate the process is not easy because Facebook is pursued quibble pending audit results from the authority in the UK, namely Information Commissioner Office (ICO).

3.8 LET'S SUM UP

Protection of the security of private data must have a place as a basic right that needs to be protected and attached to each. Such protection should not appear when data theft has occurred. The basic thing that needs to be considered and more effective is to build public awareness. The Ministry of Information and the Government of Indonesia must be able to provide and enrich people's knowledge of the importance of privacy data.

3.9FURTHER READING

- David, Robert. (2004). A dictionary of Human Rights. Europa, London, New York.
- Freeman, Marc and Gibran Van Ert. (2004). International Human Rights Law. Canada: Irwin Law Inc.
- The Institute for Policy Research and Advocacy (Elsam). (2015). Privasi 101 PanduanMemahamiPrivasi, Perlindungan Data danSurveilansKomunikasi. Norman E. Bowie, Karim Jamal. (2006).

[64]Quoted from https://www.kominfo.go.id/content/detail/13163/rudiantara-bakal-insiasiregulasi-soal-konten-medsos/0/sorotan_media.

- Privacy Rights on the Internet: Self-Regulation or Government Regulation. Business Ethics Quarterly. https://doi.org/10.5840/beq200616340
- Raymond, Wacks. (2013) Privacy and Media Freedom. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199668656.001.0001
- Westin, A.F. (1967). Privacy and Freedom. New York: Atheneum

3.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What do Articles 3 and 17 of UDHR state?**

   Article 3 and Article 17 of the Universal Declaration of Human Rights. Article 3 set the right of the person as follows: “Everyone has the right to life, freedom, and liberty as an individual. “While Article 17 to protect the freedom in two paragraphs, namely: (1) Everyone has the right to own property alone or jointly with others; (2) No one shall be deprived of his property arbitrarily. Both the terms of the Universal Declaration of Human Rights provide for the broad protection of the right to privacy.

3.11 ACTIVITY

Based on the case study provide with your opinion and solutions on how to curb such data thefts.(700-1000words)

4

Unit 4: YAHOO DATA BREACH

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Breach of 2013

4.4 Breach of 2014

4.5 Business Impact

4.6 Financial Implications

4.7 Regulatory Violations

4.8 Recommendations against hacking

4.9 Let's sum up

4.10 Further reading

4.11 Check your progress: Possible Answers

4.12 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Yahoo data breach during different times
- The impact on data breach on business
- Recommendations against hacking

4.2 INTRODUCTION

What a relief! At the end of 2016, an online service provider had announced two large data breaches involving over 1.5 billion users. Following further investigation, Yahoo announced that the cyber security breach had infected its 3 billion accounts. This is regarded as one of the most serious data leaks in the history of online service providers.[65]

Yahoo CEO Marissa Mayer's attempts to restore the company's previous success failed. Verizon announced in 2016 that it would buy Yahoo for $4.83 billion, but the sale fell apart due to Yahoo's disclosure of the data breaches. Yahoo's universe was turned upside down after it was revealed in 2014 that it had experienced data breaches. User names, email addresses, phone numbers, dates of birth, hashed keys, and certain encrypted and unencrypted security questions were stolen in the cyber-attack, which affected 500 million users. They made the public aware of the breach in 2016 and suspected it was the work of state-sponsored hackers. In an unexpected turn of events, Yahoo lodged an SEC report in early September claiming ignorance of the data breach. When a new investigation was filed in November following the official disclosure of the data leak, Yahoo admitted to learning about the hack into their scheme. Yahoo also stated in this filing that the whole attack was focused on cookies.

As Yahoo and its investigators were attempting to determine the origin and effect of the 2014 cyber-attack, they discovered a previous major attack that occurred prior to 2014. This assault occurred in the year 2013 and was attributed to an unidentified third party. The size of the attack was massive; this time, the hackers stole information from 1 billion users, including backup email addresses. The police were directed to a dark web broker who was selling the data for $300,000 in August 2015 when hunting down details of the hack.[66]

4.3BREACH OF 2013

While it is still unclear how hackers were able to steal all 3 billion Yahoo account records in 2013, an Eastern European hacking group provided the data for sale in 2016. Three organizations have acquired the data after it was put up for sale; two of

[65]See Nicole Perlroth, Yahoo Says Hackers Stole Data on 500 Million Users in 2014, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoohackers.html

[66]See Robert McMillan, Ryan Knutson & Deepa Seetharaman, Yahoo Discloses New Breach of 1 Billion User Accounts, WALL ST. J. (Dec. 15, 2016, 5:19 PM), https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts1481753131.

the identified entities are “spammers,” and the other claims to be involved in spying. Yahoo was able to track the selling of 1 billion accounts for a quarter million dollars with the help of law enforcement and an independent security agency.[67] Authorities suspect the 2013 hack was a state-sponsored attack due to the severity of the intrusion.

4.4BREACH OF 2014

Soon after Yahoo announced that 1 billion of their accounts had been hacked, another leak affecting 500 million accounts occurred. Via a spear-phishing program that directly targeted Yahoo staff, the hacker, Aleksey Belan (a Latvian hacker recruited by Russian agents), was able to obtain access to Yahoo’s User Database and account management tool. Belan mounted a workaround on a Yahoo server after gaining access to the user account, and then stole a duplicate copy of the database onto his personal computer.

Hackers used stolen cryptographic values, known as “nonces,” to create access cookies via a script built on a Yahoo server after identifying accounts of interest. The Department of Justice arrested four people for the hack in March of 2017. Russian intelligence officers made up two of the indictees. The compromised material, according to authorities, was used to spy on a variety of targets in the United States.

These major security breaches had a significant financial, corporate, and public-reputation effect on Yahoo, as well as numerous regulatory violations.

4.5BUSINESS IMPACT

The Yahoo hack revealed a variety of risks raised by the attack, not just to users and the business, but also to the entire IT world. Yahoo has effectively placed millions of consumers at risk of personal information leakage as a result of its incompetence. Yahoo took two years to notify customers, the SEC, and the general public of the security breach. Mayer, Yahoo’s CEO, was opposed to the proposal to require all affected users to update their passwords because she believed the company would lose business. As a result of this incident, Yahoo’s customers and users lost interest in the brand.

Yahoo is also accused of misleading Verizon with fake facts, leading to the signing of a stock deal with no mention of the significant security breach.[68] It gave consumers yet another excuse to think twice about doing business with Yahoo. Due to a shortage of cyber security liability insurance, it is the only company that could not be trusted with confidential data privacy and defense.

4.6FINANCIAL IMPLICATIONS

[67]See Lawrence J. Trautman, Managing Cyberthreat, 33 SANTA CLARA HIGH TECH. L.J. 230, 240 (2016) (discussing the risk assumed by companies that acquired malware-tainted Nortel software from bankruptcy proceeding); see also Lawrence J. Trautman& George P. Michaely, Jr., The SEC & the Internet: Regulating the Web of Deceit, 68 CONSUMER FIN. L.Q. REP. 262 (2014) (discussing electronic commerce operations and websites).

[68]See Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 4–6 (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323; see also SMEDINGHOFF, supra note 8, at 30–31.

During talks with Verizon, the two security events allowed Verizon to pay $350 million less for Yahoo in 2017 and sparked a slew of inquiries and litigation that tarnished Yahoo's image. Yahoo's unprecedented data theft, which exposed 3 billion users, resulted in a massive financial loss. The Securities and Exchange Commission fined them $35 million for making misleading statements about the evidence and failure to warn investors about the violation. Yahoo was ordered to pay $85 million in fines to offer free credit management services to over 200 million consumers as part of a mediation agreement. When Verizon learned of the breach, it referred to it as a "material adverse case," which cost Yahoo $350 million in merger costs. Aside from the fines, Yahoo had to pay $35 million in legal costs and another $16 million for its cyber attacks, of which $5 million was devoted exclusively to technical analysis and remediation efforts. They admitted to spending $11 million in legal fees, as well as five state and federal prosecutions and class-action cases.

4.7REGULATORY VIOLATIONS

Yahoo is accused of violating Sections 17(a) (2) and (3) of the Securities Act of 1933, as well as Section 13(a) of the Securities Exchange Act of 1934, according to the SEC's administrative order. The SEC was surprised that the violation was not disclosed quickly enough, and that investors were left in the dark for almost two years. By December 2014, Yahoo's CISO had received warnings that hundreds of millions of Yahoo users' personal information had been compromised, and they were already aware that the same group of hackers had continued to attack their database in 2015 and 2016.[69] Yahoo refused to recognize and minimize cyber security threats, which might have avoided this major data leak if it had been able to do so.[70]

4.8RECOMMENDATIONS AGAINST HACKING

A large-scale data theft is a big problem for an enterprise, and it has ramifications for both its company and its customers.[71] The following suggestions should be used to strengthen the situation and discourage companies from being hacked:
Preventive:

1. Increase data access limits by encouraging workers to only access data that they are allowed to see. Via a phishing campaign, the hacker in the 2014 breach was able to gain access to Yahoo's customer account. If multiple access authorizations are issued to different workers, one compromised employee account can do less harm based on their level of access to the

[69]Bruce H. Nearon et al., Life After Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 JURIMETRICS 379, 391, 394 (2005).

[70]"Consequences of Yahoo Data Breaches Continue." *Audit Analytics*, www.auditanalytics.com/blog/consequences-of-yahoo-data-breaches-continue/.

[71]Garum, Natt. Yahoo Says All 3 Billion User Accounts Were Impacted by 2013 Security Breach. The Verge, 3 Oct. 2017, 5:07 pm EDT, www.theverge.com/2017/10/3/16414306/yahoo-security-data-breach-3-billion-verizon

company's confidential data. In the case of Yahoo, access to the consumer website can be restricted to a limited number of high-level workers who need it.

2. Be certain that all staff and users adhere to a uniform login policy. Recommend that they update their passwords on a regular basis to keep the network and confidential data safe and to deter hackers from using the same keys to enter the device again. Yahoo's bcrypt password program can help to deter brute force attacks, but it can't prevent front door attacks. We suggest informing employees about the dangers of phishing emails and the many ways that hacks or data breaches can occur.
3. Using firewalls and encryption tools such as anti-spyware and antivirus applications, malicious code may be prevented and removed from software. Through advising consumers and staff to upgrade their systems and services on a daily basis in order to stay protected from suspected glitches and vulnerabilities. Particularly for Yahoo workers, because the vulnerabilities in their work computers could compromise the entire network.
4. Keep an eye on suspected activity or cookies: The executive branch should collaborate with the private sector to reduce or prohibit the use of cookies, as hackers have been known to use "forged cookies," which are pieces of code stored in the user's web cache that don't really need a user authentication. Utilize the tools to detect login behavior using cookies and limit access for these users in the future.
5. By supplying the security department with the necessary financial services. In the case of Yahoo, Ms. Mayer, the company's CEO, refused to provide sufficient funding for the company's technology facilities and delayed effective security protections, such as intrusion detection mechanisms for Yahoo's manufacturing systems.
6. Using specialist service services to handle IT security. Improve monitoring infrastructure by enlisting the help of trained security service providers and adhering to best practices. The IT protection department, which is located in the corporate hierarchy, is still overconfident in their own structure. The advice of a reputable IT security company will ensure the security of any sensitive corporate records.

Detective Measures:

1. Intrusion Detection System Review: Hiring an independent team or a security firm to keep an eye on the machines for suspicious activities. Reviewing any protocol violations or other prohibited behavior will aid in the prevention and diagnosis of potential risks and dangers. This will help deter intruders from obtaining access to information through viruses or malware.

Technologies for detecting security breach:

CAPTCHA stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart." It is a device that verifies that the behavior is being requested by a person. When you attempt to log into your account, the CAPTCHA will most likely appear. Words, queries, and graphics recognition are the most popular types of CAPTCHA.

reCAPTCHA: Also known as reversed CAPTCHA, this technology is used to prevent spam as well as digitize books and publications. reCAPCHA, on the other hand, uses digitized words to classify individual actions, while CAPTCHA uses random words to validate.

Since these extra measures cannot be done by computers, they can help deter robots and machines from obtaining access to secure information.

Response Measures:

1. Update account and employee credentials: When a hack is discovered, it is strongly advised that all employees change their passwords. Since the hackers have the passwords, changing the data will prevent the breach from continuing and restrict the hacker's scope. Be sure to beef up your security by enabling two-factor or multi-factor authentication, among other things.
2. The company's breach management team must use tools such as Business Impact Analysis (BIA) and Disaster Recovery to determine the scope of the breach (DR). This will assist them in identifying confidential data and taking the appropriate precautions to secure it. This team can also look at organizations that have leaked data to ensure that no one else has a copy of it.
3. Discuss a fair time to restart activities with the forensics staff and law enforcement. The forensics team will aim to carefully track the actions of users and staff because it aids in determining when the attack happened and, if activities are logged and tracked, it might be possible to detect further intrusions.

Yahoo's data theft was one to recall and respond on, but other big and small businesses are constantly at risk of being hacked. The conventional approach of focusing on vital components and defending against larger threats would not be

beneficial as the prevalent risks evolve. In today's climate, becoming pragmatic and adaptable in approaching and minimizing various threats is essential. Any employee of a company must recognize the importance of data and work to protect it from cyberattacks.It is possible if each person is informed about past attacks by someone who knows and tries to mitigate the risks. Understanding the truth is critical, and ensuring that preventive procedures are revised and in effect will guard against further threats.

4.9 LET'S SUM UP

By developing and implementing a cyber security strategy, businesses will defend themselves from future data attacks. By putting in place pre-emptive steps, certain traditional cyber security methods can be understood and put to use. Also, ensuring that all necessary updates are completed on time.Getting rid of any outdated software that are no longer in service and may be vulnerable to hacking. Keeping cyber security applications up to date and checking them to ensure they function. The most popular and reliable method is to teach staff how to create complicated codes, prevent opening attachments from phishing emails, and properly dispose of sensitive data. In the systems that are used, two-factor authentication is used. Industries should establish a bring-your-own-device policy that specifies what types of company data can be exchanged and processed on these devices. Web filtering technology, which monitors URLs in real time and blocks unwanted entry, can be used by businesses. Businesses should have a solid business continuity strategy in place to assist them through a time of turmoil. A disruption may have a negative effect on the company and revenue; providing a data backup reduces the risk.

4.10FURTHER READING

- Britannica, The Editors of Encyclopaedia. "Yahoo!" Encyclopedia Britannica.
- Al-Heeti, Abrar. "Yahoo Must Pay $50M in Damages for Security Breach." CNET, CNET, 23 Oct. 2018.
- "The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)." The National Law Review, National Law Review.
- Asher-Dotan, Lital. "Yahoo's Potential Financial Fallout Shows the Unexpected Impacts of a Data Breach." Cybereason.
- "Consequences of Yahoo Data Breaches Continue." Audit Analytics.
- Insureon. "How to Prevent a Data Breach at Your Business." Insureon.
- Williams, Martyn. "Inside the Russian Hack of Yahoo: How They Did It." CSO Online, CSO, 4 Oct. 2017.

4.11CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What kind of responsive measures can be taken into consideration?**

   This chapter discusses three solution steps, one of which is upgrading account and employee passwords. When a hack is discovered, it is strongly advised that both users update their passwords. Since the hackers have the passwords, changing the data will prevent the breach from continuing and restrict the hacker's scope. Take the requisite steps to improve your defense, such as enabling two-factor or multi-factor authentication.

4.12 ACTIVITY

Explain how the Yahoo data breach could have been avoided with proper strategies and infrastructure. (1000-1500 words)

Block-3

INDIAN LAWS AND CYBER SECURITY

1

Unit 1: PRIVACY AND CYBER LAW

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Information Privacy

1.4 Concept of Privacy

1.5 Concept of Data Protection

1.6 Privacy and Data Protection

1.7 Specific Regulatory Areas

1.8 Let’s sum up

1.9 Further reading

1.10 Check your progress: Possible Answers

1.11 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is meant by privacy
- The concept of data protection
- Specific statutory regulatory areas

1.2 INTRODUCTION

The right to privacy encompasses a wide range of issues. The right to privacy has been recognised in western culture, both legally and in everyday speech. Article 21 safeguards the right to privacy and supports human dignity. In recent years, there has been an increasing concern about the vast volume of personal information stored in electronic archives. The right to privacy applies to an individual's ability to monitor how sensitive information is collected, used, and disclosed.[72]Data information may include, but is not limited to, personal desires, behaviors, and events, family and educational records, correspondence (including mail and telephone records), medical records, and financial records. An person may be easily affected by the presence of false or deceptive computerized data about him or her that could be transmitted to an unauthorised third party at high speed and for a low cost. This increase in the use of personal data has a lot of advantages, but it also has a lot of drawbacks. Furthermore, the integration of technology has spawned a new generation of privacy and data security concerns. Personal data is readily available and communicable thanks to innovative technology. The right to privacy and data security are inherently at odds. The primary goal of data security should be to balance these competing informational desires. Individuals and organizations' data, on the other hand, should be protected in such a way that their privacy rights are not jeopardized.

1.3INFORMATION PRIVACY

The relationship between data storage and distribution technologies, the public presumption of privacy, and the legal and political concerns affecting them is known as information privacy or data privacy.[73] A few examples should be used to understand the degree to which secrecy must be preserved. The Supreme Court ruled on the issue in Union of India v. Assn. of Democratic Reforms. In a democracy, the freedom to obtain facts is recognised throughout and is a fundamental right that flows from the principle of democracy. Article 21 gives everybody the right to know, including the right to obtain information. Article 21 has a much broader reach and

[72]Sharma, Indu&Afshar, M..(2016). Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law.International Journal of Computer Applications. 145. 11-18. 10.5120/ijca2016910185.

[73]Chun Cheng Niu , Kuan Cheng Zou , Yuan Ling Ou Yang, Guan Jie Tang, Yi Zou "Security and Privacy Issues of the Internet of Things", September 2013

ambit than article 19(1). (a). The Supreme Court stated in People's Union for Civil Liberties v. Union of India that this promotes a voter's or citizen's right to know. When an individual's right to privacy and citizens' right to know compete, the former must yield to the latter because it represents the greater public good. The concern emerges as to how much information about a candidate's privacy a voter has a right to see.By eliminating the disadvantages of legislation pertaining to voters' access to information, the voter's right to hear about a candidate's privacy can be preserved and flourished. The right to monitor the exchange of publicly identifiable information about any individual is known as privacy. It necessitates a balancing mindset, as well as a balancing interest. As a result, a balanced and agreeable inter-relationship between the common good and individual liberty is needed in the end. As a result, it is concluded that a balance must be struck between a citizen's right to know and a candidate's right to privacy while seeking office.[74]

1.4CONCEPT OF PRIVACY

The concepts protection and right to privacy are difficult to grasp. It's been seen in a variety of contexts in various scenarios. 'The right to privacy is bound to include the inviolability and modesty of the body, as well as the intimacy of personal identity, including marital privacy,' according to Tom Gaiety. Jude Cooley has defined privacy as "the right to be left alone," according to the law. Edward Shils defines privacy as a "nil relationship between two or more individuals in the sense that there is no contact or connection between them, whether they want."'Once a society has made a distinction between the "outer" and "inner" man, between the life of the soul and the life of the body...the notion of a private sphere is in which man may become and remain himself,' Warren and Brandeis have eloquently explained. Privacy has been recognised in western culture, both legally and in everyday speech. However, various legal codes prioritize different facets, so it differs. Privacy is a neutral relationship that exists between individuals or entities, or between individuals and groups. Privacy is a value, a cultural state, or a situation aimed at individual and social self-realization that varies by society.

The right to freedom of speech and expression is guaranteed by the Indian Constitution, which means that an individual is free to express his or her opinion on any subject. A individual has the right to life and personal liberty, which can only be taken by legal means. Individuals and/or classes of people have an improbable right to privacy within these regulations. A person's identity is further protected against unjustified arrests, and he or she has the right to share his or her interests on the practice and propagation of either faith. Property protection is still protected because the statute allows it, i.e. a person's property cannot be taken from him without his consent.[75] Personal liberty, as defined in Article 21, has the broadest scope and

[74]AsouAminnezhad, Ali Dehghantanha, MohdTaufik Abdullah "A Survey on Privacy Issues in Digital Forensics", International Journal of cyber security and digital forensics, The society of Digital Information and wireless communication, 2012(ISSN: 2305-0012)

[75]A. A. Sattikar ,Dr. R. V. Kulkarni "A Review of Security and Privacy Issues in Social Networking", International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2784-2787.

encompasses a wide range of rights, including secrecy, sovereignty, human dignity, human property, self-evaluation, restricted and safe contact, restricting man's visibility, and so on. Any of them, such as life and personal liberty, freedom of movement, freedom of speech and expression, human and societal rights, have been elevated to the level of constitutional rights and are protected under Article 19. As such, Article 21 guarantees the right to privacy and promotes human dignity. The right to monitor the distribution and use of one's personal knowledge is referred to as privacy.[76]

1.5CONCEPT OF DATA PROTECTION

The Information Technology Act, which took effect in 2000, is the only law to date that addresses the most important aspects of data security, but not all of them. In reality, the Indian Parliament passed the Information Technology (Amendment) Act, 2008, which is the first law to have data privacy provisions. According to section 2(1)(o) of the Act, "data" refers to a formalized representation of information, knowledge, facts, concepts, or instructions that is intended to be processed, is being processed, or has been processed in a computer system or computer network, and can take any form (including computer printouts, magnetic or optical storage).[77] Personal data is not specified in the IT Act, and the concept of "data" will be more applicable in the area of cybercrime. In addition, the IT Act defines terms such as connection, computer, computer network, computer resource, computer system, computer database, records, electronic medium, electronic record, information, intermediary, secure system, and security procedure in relation to data protection. The aim of the above section is to ensure that someone who has obtained access to such information does not take undue advantage of it by releasing it to a third party without the permission of the individual concerned. The word "third-party information" is described as "any information handled by an intermediary in his capacity as an intermediary," and it's possible that this restriction even extends to "information" and "contact." Section 79 states that an intermediary is not responsible for any third-party material, data, or contact connection that he makes accessible or hastened, except under the conditions set forth in sub-sections (2) and (3).[78]

There is no concept of personal data in the IT Act. Furthermore, in the area of cybercrime, the concept of "information" will be more applicable. Data protection is a technological system of security mechanisms meant to ensure that data is treated in

[76]Mahantesh B Madiwalar, Prof(Dr.) B S Reddy "Privacy Rights and Data Protection In Cyber Space with Special Reference to E-Commerce", Global Journal for Research Analysis, Volume-4, Issue-12, Dec-2015 • ISSN No 2277 – 8160.

[77]Sanaz Taheri Boshrooyeh, AlptekinKupcu, OznurOzkasap"Security and Privacy ofDistributed Online Social Networks", Conference: IEEE ICDCS (International Conference on Distributed Computing Systems) Workshop ESP-DGC, At Columbus, Ohio

[78]Privacy and Human Rights, An International Survey of Privacy Laws and Practise, Global Internet Liberty Campaign at www.gilc.org/ privacy/survey/intro.htmlaccessedon23rd August,2013

such a way that it is protected from unauthorized, accidental, unwanted, or malicious use.

1.6PRIVACY AND DATA PROTECTION

Data regarding people should not be immediately made accessible to other individuals or organisations, according to privacy and data security laws. Each person must have a significant amount of control over the data and how it is used. Data security is a regulatory precaution that prevents the abuse of personal information on any means, even computers. That is the use of administrative, electronic, or physical barriers to protect sensitive information. Data security and privacy are inextricably linked. Data about a person, such as his name, location, phone numbers, occupation, relatives, choices, and so on, can be found in a variety of locations, including schools, universities, banks, directories, polls, and numerous web pages. Passing such information on to third parties will result in invasions of privacy, such as constant marketing calls. The Information Technology (Amendment) Act, 2008 enumerates the main rules on privacy and data security, including identifying data, civil and criminal responsibility for data breaches, and confidentiality and privacy violations.

1.7SPECIFIC REGULATORY AREAS

1.7.1 Financial privacy

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983[79]

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except in accordance with laws of practice and usage.

The Prevention of Money Laundering Act 2002[80]

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offence under the PMLA.

Credit Information Companies (Regulation) Act 2005 and The Credit Information Companies Regulations 2006[81]

[79] http://legislative.gov.in/sites/default/files/A1983-48_0.pdf.
[80] https://dea.gov.in/sites/default/files/moneylaunderingact.pdf
[81] http://legislative.gov.in/sites/default/files/A2005-30.pdf.

This legislation is essentially aimed at regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offences is maintained permanently while information relating to civil offences is retained for seven years from the first reporting of the offence. In fact, the regulations also prescribe that personal information that has become irrelevant may be destroyed, erased or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For the purpose of redressal, a complaint can be written to the Reserve Bank of India.

Payment and Settlement Systems Act 2007[82]

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

Foreign Contribution Regulation Act 2010[83]

This Act is aimed at regulating and prohibiting the acceptance and utilisation of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

Workplace privacy

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, in relation to the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

Children's privacy

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child's best interest. The Personal Data

[82] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf
[83] https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf

Protection Bill 2019 provides for the protection of personal and sensitive data of children by requiring consent of a parent or guardian and imposing various restrictions on data fiduciaries processing such data.

Health and medical privacy

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)[84] regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

Medical Termination of Pregnancy Act 1971

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

Ethical Guidelines for Biomedical Research on Human Subjects

These Guidelines require investigators to maintain confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is risk to public health.

1.7.2 Technological innovation and privacy law

There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation. The Personal Data Protection Bill 2019 does prohibit data fiduciaries from profiling, tracking or behaviourally monitoring, or generating targeted advertising at children.

The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle and process data, and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.[85]

1.8 LET'S SUM UP

Privacy is a fundamental human right, and computing networks store vast quantities of potentially sensitive data. Unauthorized access to a device, computer system, computer network, or services, unauthorized alteration, elimination, extension, change, degradation, replication, or transfer of records, computer database, and so on are all covered by Chapters IX and XI of the Information Technology Act. Financial records, health information, company plans, intellectual property, and personal data could all be protected. However, today's technology allows anybody to

[84] http://niti.gov.in/writereaddata/files/1.pdf

[85] The sources upto this level are available at https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india

access all information about anyone from anywhere at any moment, posing a new vulnerability to private and sensitive data. Technology has gained worldwide recognition as a result of globalization. Different nations have adopted different regulatory frameworks from time to time, such as the DPA (Data Protection Act) 1998 in the United Kingdom, the ECPA (Electronic Communications Privacy Act of 1986) in the United States, and so on. Unique privacy regulations apply in the United States to preserve student school data, children's online privacy, medical records, and private financial documents. Self-regulatory initiatives in both countries are assisting in the definition of better privacy environments. The right to privacy is protected by the Constitution, but its expansion and extension is solely at the discretion of the courts. It is exceedingly impossible to avoid information from leaking into the public domain in today's wired society if anyone is willing to do so without resorting to extremely repressive tactics. The Information Technology (Amendment) Act, 2008 dealt with data security and privacy, but not in a comprehensive way. The Information Technology Act would define strict guidelines for the processes and purposes of assimilation of the right to privacy and personal data. To sum up, the IT Act has an issue with data security, and separate regulation is desperately needed to strike an acceptable balance between personal liberty and privacy.

1.9FURTHER READING

- Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233.
- Edward Shils, "Privacy: Its Constitution and Vicissitudes" 31 Law & Contemporary Problems 281 (1966).
- Samuel Warren & Louis D. Brandeis, "The Right to Privacy" Harvard Law Review 193 (1980).

1.10CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How can data protection be effectively ensured in India?**

   The right to privacy is protected by the Constitution, but its expansion and extension is solely at the discretion of the courts. It is exceedingly impossible to avoid information from leaking into the public domain in today's wired society if anyone is willing to do so without resorting to extremely repressive tactics. The Information Technology (Amendment) Act, 2008 dealt with data security and privacy, but not in a comprehensive way. The Information Technology Act would define strict guidelines for the processes and purposes of assimilation of the right to privacy and personal data.

1.11 ACTIVITY

Explain the concept of data protection with respect to the Information Technology Act, 2000. (1000-1500 words

Unit 2: DATA PROTECTION BILL 2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Anonymised Data

2.4 Consent

2.5 Right to be Forgotten and Right of Erasure

2.6 Rights of Data Principal: Reporting of Personal Data Breach

2.7 Data Protection Bill: Brief Analysis

2.8 Let's sum up

2.9 Further reading

2.10 Check your progress: Possible Answers

2.11 Activity

2.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- The provisions relating to the Data Protection Bill
- Protection of personal data and the effects of breach of personal data
- About anonymised data

2.2 INTRODUCTION

"Data is the new oil…."—Clive Humby

The above statement was made in the year 2006 and almost a decade later, it rings true in the present day information technology context. "Data" has become one of the most important, if not the most important resources every individual holds in 2019. In light of its importance, data has also become subject to theft and misuse. Countries, having realised its value, have started formulating laws and regulations to protect from any form of misuse and developed countries have already formed stringent enforcement mechanisms to protect data at the same level as its citizens. Data has come across more than just a container of information. In an article published in 2017 aptly puts, "internet companies' control of data gives them enormous power. Old ways of thinking about competition, devised in the era of oil, look outdated in what has come to be called the 'data economy'."[86]

Apart from the Information Technology Act, 2000, dealing with issues of cybercrime and e-contracts, India does not have any legislation governing data protection. The Supreme Court's recommendation for much-needed legislation on data protection in India in K.S. Puttaswamy v. Union of India or the "right to privacy" became the foundation for formulating a new law on the subject. Justice B.N. Srikrishna led Committee of Experts submitted a report on the same and the Draft Personal Data Protection Bill, 2018 (2018 Data Protection Bill). The Draft Personal Data Protection Bill made the rounds with regard to its formulation being hugely inspired by the European Union's General Data Protection Regulation (GDPR) in terms of data localisation, expansion of the definition of "sensitive personal data", among other things. Upon receiving various reviews and recommendations from the stakeholders of various levels, the Ministry of Electronics and Information Technology prepared the 2019 Bill (the Personal Data Protection Bill, 2019) which was introduced to the Lok Sabha on 11-12-2019. The 2019 Bill is primarily based upon its predecessor with certain significant changes. As much as it has done away with certain flaws of the 2018 Data Protection Bill, the 2019 Bill is also inclusive of red flags raising questions regarding the personal rights of the individuals or "data principles". This article focuses on discussing some changes in the newly proposed Bill and the grey areas

[86]Sable, Vivek.(2020). Constitutional Validity of Data Protection Bill 2019.

in the provisions. The article shall also briefly provide a comparative analysis of the said Indian provisions with GDPR.[87]

2.3ANONYMISED DATA

The term "anonymised records" is one of the first provisions of the 2019 Data Protection Bill that seems to be contradictory. Clause 3 defines the term "anonymisation" in a very specific way. "Anonymisation in relation to personal data" means "any permanent method of transferring or translating personal data to a manner in which a data principal cannot be traced, and which satisfies the authority's requirements of irreversibility."The Act prohibits the processing of anonymised data, but Clause 91 of the proposed Bill makes an exception, allowing the Central Government to collect anonymised data or other non-personal data for "targeting or delivery of services, or the formulation of evidence-based policies." This provision needs further more robust enforcement mechanism along with necessary regulations regarding the usage of such anonymised data.[88]
A privacy bill brings all sectors to abide by the tenets of data security. Except, under the new Bill, that does not quite happen. This is because provisions are very strong when it comes to how private companies and the other entities collect and process data but it lacks when it comes to how the Government can access personal data.

2.4CONSENT

A provision on the requirement of explicit consent before processing of personal data has been provided in Clause 11 of the 2019 Data Protection Bill. However, the grounds for the processing of personal data without consent in certain cases as provided under the later clauses eventually ends up limiting the power of Clause 11 due to the vast number of exceptions.

2.5RIGHT TO BE FORGOTTEN AND RIGHT OF ERASURE

As mentioned above earlier, even despite new additions to the 2019 Data Protection Bill, it falls short to provide complete justice to the rights of the data principal, among other things. It is very interesting to note one such addition in the new Bill is providing the data principal for the "right of erasure" of personal data which is no longer necessary.[89] Clause 18 of the 2019 Data Protection Bill reads: The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such

[87]The Economic Times. (2019). Personal Data Protection Bill: India's digital safety kit. [online] Available at: https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-indias-digital-safetykit/articleshow/72429680.cms?from=mdr
[88]Harvard Business Review. (2019). How India Plans to Protect Consumer Data. [online] Available at: https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data
[89]India Today. (2019). Personal Data Protection Bill seeks access to user data without consent in select cases: Report. [online] Available at: https://www.indiatoday.in/india/story/personal-data-protection-bill-seeks-accessto-user-data-without-consent-in-select-cases-report-1627265-2019-12-11

conditions and in such manner as may be specified by regulations, have the right to—
(a) the correction of inaccurate or misleading personal data;
(b) the completion of incomplete personal data;
(c) the updating of personal data that is out of date; and
(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.
The 2019 Data Protection Bill has simply expanded the provision by including rights for completion, updating and erasure of personal data which the 2018 Draft Bill, in comparison, only provided for the right to correct personal data. Although in the sub-clauses to Clause 18 it lays down the procedure on how the data principal will be able to perform the necessary tasks, it will still require a detailed regulation. It will also be interesting to note that Clause 9 of the 2019 Data Protection Bill provides for the deletion of such data by the data fiduciary which is no longer necessary, but it does not provide any system for notifying the data principal regarding the same.
When it comes to the aspect of "right to be forgotten", the Indian regime has provided it separately under two different clauses unlike the GDPR, where the "right to be forgotten" and "right to erasure" is provided under one article. Despite a new addition of "right of erasure", the 2019 Data Protection Bill still retains one of the major flaws of the 2018 Draft Bill with certain minimum modifications. The 2018 Draft Bill camouflaged the full exercise of the right by stating that the data principal shall have the "right to restrict or prevent continuing disclosure of personal data", which was clearly ambiguous in nature. Clause 20 of the proposed Bill does not shift much from the abovementioned words, thereby retaining the earlier criticised provision. The proviso to the clause states that "no order shall be made under this sub-clause unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen." This is one of the most prominent examples to show why Indian courts have a plethora of cases pending. Especially in the 21st century, where data is considered more valuable than any other asset, and by the time the matter will be heard by the judiciary the data principal would not be in a position to proceed with his case. To add to the above, the enforcement of the data principal's right to "restrict or prevent continuing disclosure of personal data" vests upon the discretion of the adjudicating officer. In this context, not only does the GDPR provide clarity regarding erasure of personal data, it provides for a wider set of provisions to obligate the data controller in the erasure of the data. Therefore, this proves to be another provision which lacks clarity as to the rights of the data principal.

2.6RIGHTS OF DATA PRINCIPAL: REPORTING OF PERSONAL DATA BREACH

The highly criticised, Draft Bill, presented a bizarre provision wherein it provided that in case of breach of personal data, neither the data fiduciary nor the data protection authority shall have any obligation or any requirement to inform the data principal about the breach. Hoping this will be dealt more strategically in lines with the GDPR, the 2019 Data Protection Bill fails to come up with any change. The provision presents itself in the exact format in the new Bill and there is a very limited requirement for the data fiduciary or the data protection authority to notify

the data principal regarding the breach. The provision also provides for the data protection authority the right to publish such breach on their website but retains the right to inform the data principal on its own accords, thereby exposing the data principal to a large number of leaks of his personal data and thereby its misuse. It is one of the provisions which needs significant attention in light of the recent data breaches occurring within the nation. The 2019 Data Protection Bill also fails to provide for a system capable of countering such breach of data in a well-equipped manner. The mechanism is merely a notification of such breach to the necessary websites and other platforms. The GDPR, under Article 34 provides for a more stricter regime wherein it has explicitly provided for notification to the data subjects ("data principal" in Indian context) regarding any such breach of personal data and in case where it has not been communicated in due time by the data controller ("data fiduciary" in Indian context), the authority, upon considering the likelihood of such breach shall notify to the data subject. Since the Indian Data Protection Bill is largely based upon the GDPR, it is indeed surprising to note such important criteria have been left out of the regime.

2.7DATA PROTECTION BILL: BRIEF ANALYSIS

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose. Consent must be obtained before collection of the data. The IT Rules also mandate that sensitive personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified. The Personal Data Protection Bill 2019 defines 'consent' and 'explicit consent' and provides grounds, including the functions of the state, or compliance with a court order, for the lawful processing of personal data as well as sensitive personal data.

Purpose limitation

The IT Rules state that any information collected by a body corporate or a person on its behalf shall be used for the purpose for which it has been collected. The Personal Data Protection Bill 2019 prescribes that personal data be processed only for specific, clear and lawful purposes. It states that data shall be processed in a fair and reasonable manner that ensures the privacy of the data principal (the person to whom the data relates) and for the purpose consented to by the data principal. Alternatively, the purpose may be incidental to or connected with such purpose, and for which the data principal would reasonably expect that such personal data shall be used. It also limits the collection of personal data to such data that is necessary for the purposes of processing.

Data retention

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such period of time as prescribed by the central government. The Personal Data Protection Bill 2019 states that a data fiduciary may not retain personal data beyond the period necessary to satisfy the purpose for which it is processed. It also states that such data must be deleted at the end of this period. However, the Bill also allows for longer periods of retention if required by compliance with legal obligations, or if the consent of the data principal has been obtained, and prescribes periodic reviews by data fiduciaries for an ongoing assessment of the continued necessity of the retention of personal data.

Registration formalities

India currently does not have any legislative requirements with respect to registration or notification procedures for data controllers or processors. The Personal Data Protection Bill 2019 requires that based on certain criteria, the data protection authority envisaged by the bill shall notify certain data fiduciaries as being 'significant'. Significant data fiduciaries will be required to register with the authority in a manner specified by it, and will also be subject to data protection impact assessments, data audits, etc. The Bill also states that the data protection authority may require registration by other data fiduciaries at its discretion, even if such entities are not 'significant'.

Rights of individuals

Access to data

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided. The Personal Data Protection Bill 2019 teases out this right in more detail, providing the option for the data principal to obtain from the data fiduciary in a clear and concise manner, confirmation of whether its personal data is being (or has been) processed and a brief summary of processing activities. The Bill states that the data principal shall also have the right to access in one place the identities of the data fiduciaries with whom their personal data has been shared, along with the categories of such personal data.

Correction and deletion

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

The Personal Data Protection Bill 2019 provides data principals with the right to correction and erasure of personal data. However, such correction or erasure is subject to the agreement of the data fiduciary. If there is a dispute between the two entities in this regard, the data principal may require the data fiduciary to indicate alongside the relevant personal data that it has been disputed by the data principal.

Objection to processing and marketing

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent that may have been given to the corporate entity previously, and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the corporate body is prohibited from processing the personal information in question. In the case of the data subject not providing consent, or later withdrawing consent, the corporate body shall have the option not to provide the goods or services for which the information was sought.

The Personal Data Protection Bill 2019 also envisages the right to be forgotten, in that it provides for the data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary. However, this right may only be enforced by order of an Adjudicating Officer.

The Supreme Court of India has also identified and clarified that citizens have the right to be forgotten, which exists in physical and virtual spaces such as the internet, under the umbrella of informational privacy.

Right to restrict processing

As mentioned above, the Personal Data protection Bill 2019 provides for a data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary, but only if the data protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure have been found.

Right to data portability

The IT Act and Rules do not contain provisions relevant to data portability. However, the Personal Data protection Bill 2019 provides data principals with this right where processing has been performed through automated means. Subject to certain restrictions, the data principal shall have the right to receive in a structured, commonly used and machine-readable format, any personal data provided to the data fiduciary, the data that has been generated in the course of provision of services or use of goods by such fiduciary, or the data that forms part of the profile on the data principal, or that the data fiduciary has otherwise obtained.

Right to withdraw consent

The Personal Data Protection Bill 2019 envisages the right to withdraw consent, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

Disclosure of data

Data subjects also possess rights with respect to disclosure of the information they provide. Disclosure of sensitive personal information requires the provider's prior permission unless either disclosure has already been agreed to in the contract between the data subject and the data controller; or disclosure is necessary for compliance with a legal obligation.

The exceptions to this rule are if an order under law has been made, or if a disclosure must be made to government agencies mandated under the law to obtain information for the purposes of verification of identity; prevention, detection and investigation of crime; or prosecution or punishment of offences.

Recipients of this sensitive personal information are prohibited from further disclosing the information.

Right to complain to the relevant data protection authority

Rule 5, subsection 9 of the IT Rules mandates that all discrepancies or grievances reported to data controllers must be addressed in a timely manner. Corporate entities must designate grievance officers for this purpose, and the names and details of said officers must be published on the website of the body corporate. The grievance officer must redress respective grievances within a month from the date of receipt of said grievances.

The Personal Data Protection Bill 2019 states that the data fiduciary must provide all data principals with clear information on the procedure for grievance redressal under the Bill. Under the Bill, a data principal may make a complaint of contravention of any provision of the Bill to the data protection officer (in the case of a significant data fiduciary) or any other officer designated for this purpose (in the case of any other data fiduciary). Should such officer fail to resolve the complaint expeditiously and within 30 day of receipt of the complaint, the data principal may file a complaint with the data protection authority.[90]

2.8 LET'S SUM UP

The 2019 Data Protection Bill has brought about certain important additions. Namely, the "social media intermediaries", "sandbox for encouraging innovation", etc. However, it is safe to say most of the important red-flagged provisions of the 2018 Draft Bill still remain, thereby the new proposed Bill simply can be called an "old wine in a new bottle". Most of the provisions lack clarity and proper enforcement mechanism, which if passed as an Act, would end up increasing volumes of petitions and most certainly be raising questions regarding the security of an individual's personal data. Upon comparing the Indian regime with the GDPR, it can be safe to say that where the latter seeks to focus on the protection of the data principal's rights, the former puts more emphasis on authority and fiduciary's rights. It will be interesting to see what the joint selective committee responds upon reviewing the new Bill. As mentioned above, data is the most valuable asset in today's time, and misuse of the same will lead to doomsday for the individuals, and eventually the country.

2.9FURTHER READING

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna the Personal Data Protection Bill, 2018<http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report comp.pdf>, the Personal Data Protection Bill, 2018

[90]https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india

<http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf>;.

- European Union's General Data Protection Regulation [Regulation (EU) 2016/679] <https://gdpr-info.eu/>.
- <https://www.indiatoday.in/india-today-insight/story/data-protection-bill-govt-breaks-silence-but-secrecy-remains-1627717-2019-12-12>.

2.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Does the new Data Protection Bill favour the right to be forgotten?**

   When it comes to the aspect of "right to be forgotten", the Indian regime has provided it separately under two different clauses unlike the GDPR, where the "right to be forgotten" and "right to erasure" is provided under one article. Despite a new addition of "right of erasure", the 2019 Data Protection Bill still retains one of the major flaws of the 2018 Draft Bill with certain minimum modifications.

2.11 ACTIVITY

Explain the provisions of Data Protection Bill which talk about the anonymised data. (1000-1500 words)

Unit 3: CYBER CRIMES AND THE LAW: EVALUATION OF THE INFORMATION TECHNOLOGY ACT, 2000

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Concept of Cyber Terrorism

3.4 Cyber Criminals

3.5 Positive Aspects of IT Act, 2000

3.6 Negative Aspects of IT Act, 2000

3.7 Let's sum up

3.8 Further reading

3.9 Check your progress: Possible Answers

3.10 Activity

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- The concept of cyber terrorism
- About who are the cyber criminals
- About the evolution of the Information Technology Act, 2000

3.2 INTRODUCTION

Knowledge is a resource that is worthless until it is retrieved, stored, and put to good use. Information technology is concerned with data collection, access, processing, interpretation, and intelligent decision-making. Information technology encompasses the processes and devices that allow the production, collection, processing, storage, display, and distribution of information. Individually and as a culture, information technology has an impact.[91]

The hardware and software of a computer and telecommunication system are the foundations of information technology. This, though, is just one aspect of information technology. The other facets are today's global threats, such as cybercrime and, most importantly, cyberterrorism. When the internet was first created, the founders had no idea that it would grow into an all-encompassing revolution that could be used for illegal purposes and necessitate regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level the examples of it are:

(i) Cyber stalking
(ii) Cyber harassment
(iii) Cyber fraud
(iv) Cyber defamation
(v) Spam
(vi) Hacking
(vii) Trafficking
(viii) Distribution
(ix) Posting and dissemination of obscene material including pornography
(x) Indecent exposure and child pornography, etc.

The misapplication of technology has necessitated the enactment and enforcement of cyber rules.[92] The machine has grown in importance in every part of our lives since the new millennium has begun. This involves the use of computers by those engaged in criminal activity. Computers now play a significant part in nearly any crime committed. While not all crime committed is a computer crime, it does mean that law enforcement must become even more computer literate in order to keep up with the criminal aspect."For the first time in human history, algorithms and digital systems make it possible to own, not just execute, a crime," writes Donn Parker. Today, a total fraud in software can be passed from one perpetrator to the next, with

[91]Basu, Subhajit& Jones, Richard. (2005). Indian Information and Technology Act 2000: review of the Regulatory Powers under the Act. International Review of Law Computers & Technology. 19. 209-230. 10.1080/13600860500133495.

[92]S Basu and R Jones 'Legal issues affecting e-commerce: a review of the Indian Information Technology Act 2000', Contemporary South Asia Vol 12(1), 2003.

each refining or modifying it to his or her own needs." However, the issue of whether these cyber regulations are capable of controlling cyber crime operations demands the most consideration.[93]

Many information technology (IT) experts were unaware of and uninterested in the cybercrime epidemic until recently. In certain ways, law enforcement agents lacked the resources they needed to deal with the problem; outdated rules didn't quite suit the offenses being committed, recent laws hadn't quite caught up to reality, and there were few judicial precedents to look to for direction. Furthermore, privacy debates hindered law enforcement's efforts to collect the facts required to investigate these new cases. Finally, there was some animosity—or at the very least, mistrust—between the two most important actors in any fruitful battle against cyber crime: law enforcement agents and tech experts. However, if we want to monitor the cyber crime issue and make the internet a secure "place" for its users, strong coordination between the two is necessary.

Law enforcement officers are familiar with the criminal culture as well as the fundamentals of collecting evidence and getting criminals to justice. IT professionals are familiar with computers and networks, as well as how they operate and how to locate information about them. Each of them has half of the solution to the cyber criminal's problem. IT experts need clear definitions of cybercrime in order to determine who (and what) to refer to the police, but law enforcement officers need formal definitions of particular offences in order to prosecute a suspect. The first step in identifying individual cyber criminals is to organize all of the activities that may be classified as cyber crimes into groups.[94]

3.3CONCEPT OF CYBER TERRORISM

Both cyber fraud and cyber terrorism are offences committed online. However, there is a distinction between the two in terms of the perpetrator's motivation and purpose. While a cyber crime may be loosely described as an illegal act in which a device is used as a weapon, a target, or both, cyber terrorism requires a more comprehensive description. Cyber terrorism may be described as the premeditated use of disruptive activities, or the threat of disruptive activities, in cyberspace with the intent to further social, ideological, moral, political, or related goals, or to threaten someone in the process.[95]

3.4CYBER CRIMINALS

An convict or a suspect is someone who does something wrong with the intent of committing a felony. Any one who commits a cyber crime is referred to as a cyber criminal in this case. Children and teenagers aged 6 to 18 years may be cyber

[93]Y Benkler 'A free information ecology in digital environment', New York University Conference, Session 12, The Information Law Institute at New York University School of Law, 2001, at p 29

[94]S Wilske and T Schiller 'International jurisdiction in cyberspace: which states may regulate the Internet?', Federal Comm. Vol 50, LJ 117, 1223 –3, 2001.

[95]'Cyber crime and punishment? Archaic laws threaten global information', Mcconnell International December, 2000. Available at: http://www.mcconnellinternational.com/services/ cybercrime.htm

criminals; they may be organized terrorists, skilled hackers or crackers, disgruntled workers, cheaters, or even psychics.

(a) Kids and teenagers (Age group 9-16)

While it is impossible to imagine, it is accurate. Teenagers make up the majority of inexperienced hackers and cyber criminals. Hacking through a computer machine or a website is a source of pride for them, who have just recently started to learn what seems to be a great deal about technology. There's also the issue of looking extremely intelligent among peers. This teenage insurgents can even engage in cybercrime without being aware that they are doing so.

Teen hackers, according to the BBC, have progressed from just seeking to make a name for themselves to potentially finding their way through a life of crime through the use of computers. One of the most significant developments in 2004 was the waning power of the boy hackers eager to make a name for themselves by writing a fast-spreading virus, according to Kevin Hogan. While teen virus authors will continue to experiment with malicious programming, illegal use of malicious programs increased significantly in 2004. The use of technologies by criminals was fueled by financial rewards.[96]

Another cause for the rise of juvenile criminals in cybercrime is that many offenders, often young college students, are ignorant of the severity of the crime. An engineering college student from Tamil Nadu was recently arrested by the Chennai City Police for sending an unsolicited message to a chartered accountant. The young man has been released on bond. As a result, counseling sessions for college students must be established in order to inform them about the seriousness of such offences and the repercussions that can result.

(b) Organised hacktivists

Hacktivists are hackers who have a specific (usually political) goal in mind. In other instances, the cause may be civic justice, religious activism, or something else else. Attacks by a group of hackers known as the Pakistani Cyber Warriors on roughly 200 popular Indian websites are a fine example of political hacktivists at work.

(c) Disgruntled employees

It's hard to imagine how vengeful disgruntled workers can be. They had the choice of going on strike against their employers up to now. Disgruntled workers can now cause more damage to their bosses by committing tech-related offences, and can tear whole networks down, thanks to increased computer freedom and process automation.

(d) Professional hackers (Corporate espionage)

Company organizations now store much of their records in electronic form as a result of extensive computerization. Hackers are used by rival organizations to capture industrial secrets and other intelligence that may be useful to them. The temptation to employ sophisticated hackers for industrial espionage stems from the fact that physical presence is no longer needed to obtain access to critical documents if hacking can procure them.[97]

---

[96] L Lessig Code and Other Laws of Cyberspace, Basic Books, 1999, at p 6; for the contrary view see D Post 'What Larry doesn't get: code, law and liberty in cyberspace', Stanford Law Review Vol 52, 2000, at p 1439.

[97] U Sieber 'Legal aspects of computer-related crime in the information society', Comcrime study prepared for the European Commission 19 January, 1998. Available at: http://europa.eu.int/ ISPO/legal/en/comcrime/sieber.doc

3.5POSITIVE ASPECTS OF THE IT ACT, 2000

Even an email was not recognised as an accepted civil means of correspondence or as testimony in a court of law prior to the passage of the Information Technology Act of 2000. However, the IT Act of 2000 modified this situation by recognizing the electronic version as a legal format. The Information Technology Act of 2000 is, without a doubt, a move forward.

Companies will be required to conduct electronic trading using the regulatory infrastructure established by the IT Act of 2000, from the viewpoint of the private sector. The development of electronic commerce in India was hampered before the Indian cyber law took force because there was no legal infrastructure in place to control commercial transactions conducted online. Corporate transfers will soon be able to be completed electronically using digital signatures. The IT Act of 2000 has granted these digital signatures legal status and sanction.

In today's world, businesses archive records on their own operating systems and keep a backup. Companies will also have a contractual solution if anyone hacks into their operating systems or networks and causes disruption or copies records, thanks to the IT Act of 2000. The IT Act of 2000 provides a relief in the form of punitive damages in the amount of Rs 1,000,000 in compensation.

The Information Technology Act of 2000 defines a variety of cyber crimes, including hacking and computer code damage. Prior to the implementation of the Indian cyber rule, businesses were powerless because there was no legal recourse for such problems. The IT Act of 2000, on the other hand, completely transformed the landscape.

3.6NEGATIVE ASPECTS OF THE IT ACT, 2000

The IT Act, 2000 is likely to cause a conflict of jurisdiction.

Domain names are the foundation of electronic commerce. The Information Technology Act of 2000 makes no mention of domain names. Also domain names have not been specified, and domain name owners' rights and liability are not included in the legislation.

The Information Technology Act of 2000 does not address any questions relating to the enforcement of intellectual property rights in the online world. The statute has left many gaps by leaving contentious but crucial problems such as internet copyrights, trade marks, and patents unaddressed.

When the legislation governing cybercrime evolves, so do the new modes and types of cybercrime. The list of offenses identified in the IT Act of 2000 is far from exhaustive. However, the applicable provisions of the IT Act, 2000 are written in such a way that they seem to be the only cyber offenses that are conceivable and occur. The Information Technology Act of 2000 does not contain a variety of cyber and internet-related offences. These include:

(a) Theft of internet hours
(b) Cyber theft
(c) Cyber stalking
(d) Cyber harassment
(e) Cyber defamation
(f) Cyber fraud
(g) Misuse of credit card numbers

(h) Chat room abuse

Several critical concerns relating to the e-commerce domain, such as anonymity and content control, were not addressed by the IT Act of 2000. The topic of privacy has been completely ignored. Another ambiguity of the IT Act is that it makes no mention of antitrust concerns.

The enforcement of the Indian cyber law is the most serious problem. The IT Act of 2000 does not have any guidelines for enforcement. Furthermore, given India's low internet penetration and the fact that most government and police officials are not tech savvy, the latest Indian cyber law poses more questions than it addresses. To eliminate the above-mentioned grey areas, it appears that Parliament will need to update the IT Act of 2000.

3.7 LET'S SUM UP

It is necessary to pass new laws that cover all facets of cybercrime in order to eliminate legal ambiguities. The recent blasts in Ahmedabad, Bangalore, and Delhi highlight the danger that cyberspace practices pose to humanity, and we agree that only technology and its widespread use can effectively combat these issues. The government should take reasonable measures to limit the content that is readily available for download. The IT Act of 2000 should be updated to make it more accessible and effective in combating crime. Training and public awareness activities can be implemented in the private and public sectors. In India, the number of cyber cops should be increased. The jurisdiction issue is present in the enforcement phase, which can be resolved because cyber criminals have no jurisdiction limit, so why do the laws exist? After all, the laws are in place to punish the criminals, but the current situation allows them to flee.

In today's world, there is a need to develop a "cyber-jurisprudence" that can be used to test and criticize "cyber ethics." There is also a pressing need to develop a cyberspace code of ethics and discipline. The Information Technology Act of 2000 was enacted in response to the country's growing cybercrime crisis. Since the internet is a conduit for vast amounts of data and a vast network of communications around the globe, it is important to exercise vigilance when using it. As a result, it is important to teach everybody and practice secure coding in order to avoid cybercrime.

Many other programmers, including Frank William Abagnale and Robert Morris, want to put their hacking expertise to greater use. This practice is still going on today, with businesses hiring genius hackers as intelligence researchers. There is also a pressing need to develop a cyberspace and discipline code of ethics. It is impossible to determine fault in cyberspace using conventional criminal law standards. Since the majority of cyber offenders are under the age of majority, a new legislative system to deal with them must be developed. Since the cyber universe has no borders, enacting rules to protect all aspects is a Herculean task. However, a balance must be achieved, and legislation must be developed to combat cybercrime.

3.8FURTHER READING

- Tom Gaiety, "Right to Privacy" 12 Harvard Civil Rights Civil Liberties Law Review 233.

- Edward Shils, “Privacy: Its Constitution and Vicissitudes” 31 Law & Contemporary Problems 281 (1966).
- Samuel Warren & Louis D. Brandeis, “The Right to Privacy” Harvard Law Review 193 (1980).

3.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What are the negative aspects of IT Act?

The Information Technology Act of 2000 does not address any questions relating to the enforcement of intellectual property rights in the online world. The statute has left many gaps by leaving contentious but crucial problems such as internet copyrights, trademarks, and patents unaddressed.

3.10 ACTIVITY

Elaborate the types of Cyber Criminals. (1000-1500 words)

Unit 4: CYBER STALKING AND THE PLIGHT OF WOMEN IN INDIA — A LEGAL PERSPECTIVE

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Understanding Cyber Stalking & Its Impact

4.4 Cyber Stalking: Legal Remedies

4.5 Let's sum up

4.6 Further reading

4.7 Check your progress: Possible Answers

4.8 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- What is known as cyber stalking
- Legal remedies for cyber stalking
- How women can be victimised for cyber stalking

4.2 INTRODUCTION

In June 2016, in Salem district of Tamil Nadu, a 21-year-old woman saw a picture of her face, digitally superimposed on the body of another woman, posted on a social networking site. She informed her parents, and also identified the man responsible for it. He allegedly warped her image using a cell phone app, posted it to the site, and tagged her in the post after she allegedly refused his marriage proposal.[98] A report was filed with the Cyber Crime Cell by the woman's parent. She discovered another blurred picture tagged to her social networking site a few days later, this time with her name and her father's phone number. The woman committed suicide on the same day. In her suicide note, she expressed her complete ignorance about the distorted images and her failure to convince anybody.

With a significant increase in the usage of computer in our daily life and advancement of information technology, the vulnerability for users of computer and internet has remarkably gone up in the cyberspace today. If technology progresses, the vast technological potential of modern computers/computing machines creates possibilities for exploitation as well as criminal activity. Unfortunately, many people are unaware of the bugs they are vulnerable to when surfing the internet, posting on social networking sites, or saving data on their computers. At the same time, perpetrators use the cyberspace as a platform for indulging in various criminal activities against the users. In fact, traditional offences such as rape, molestation and different forms of sexual abuse have gained new significance due to the development of information and communication technology.

There are incidences of rape scenes in the mobile phone devices, extraction of money by threatening to publish images/videos relating to the same. The Information Technology Act, 2000 (hereinafter known as IT Act, 2000) has recognized various offences relating to cyberspace. Among many offensive acts on cyberspace, online abuse is a common phenomenon all over the world, which has directly or indirectly affected online users of different age groups leading to different forms of harassment such as gender bullying, trolling, stalking etc. A person's repetitive, unsolicited, malicious behavior across cyberspace with the intent to terrify, bully, humiliate, insult, taunt, or stalk someone else is known as cyber harassment. Apart from the physical act of harassment being considered as an offence under the Indian laws, any harassment caused through electronic media such as social networking sites, chat rooms, e-mail etc. is also considered to have similar impact as far as traditional

[98] Abhiraj Thakur, Cyberstalking: A Crime or A Tort, Jun. 21, 2016

offences of harassment are concerned.[99] According to popular perceptions, women in India make most vulnerable targets on the internet and digital communication technology due to their gender and consumability of images of Indian women as subject matter of pornography. On many occasions, women become the target of such abnormal activities to destroy the image of the immediate family members. However, it is unfortunate that multiple cases go unreported either due to lack of awareness or absence of stringent laws to deal with them. It is also interesting to note that there are a very few cases of this nature which are actually registered and prosecuted.[100] Besides, with the striking down of Section 66A of the Information Technology Act, 2000 in the decision of the Supreme Court in Shreya Singhal v. Union of India, there has been a void in law to respond to such offences. Highlighting on the fundamental right to freedom of speech and expression, the judgment held that liberty of thought and expression is not merely an inspirational ideal. It is also "a cardinal value that is of paramount significance under our constitutional scheme." Under such a paradoxical situation, where the legal fraternity insists on upholding right to freedom of speech and expression on the one hand and use of cyberspace for publishing offensive messages/images about women (which also includes stalking) on the other hand, it becomes pertinent to understand the phenomenon of cyber stalking, its impact on women and the various challenges involved in effectively addressing this menace.[101]

4.3UNDERSTANDING CYBER STALKING & ITS IMPACT

A. Concept of Cyber Stalking

Stalking has emerged as a socio-legal problem of the recent time, which has resulted in its incorporation as criminal offence in the Indian laws. According to the Oxford Dictionary, stalking means "pursuing stealthily". In other words, stalking refers to trailing someone with the intent of harassing or inconveniencing them. Stalking is characterized as repetitive and unwelcome harassing behavior that is aggressive and intentionally aimed at a single individual (the victim), and that would lead a rational person to fear physical harm or death for themselves or family members.[102]
Stalking may be characterized by the following:

- A repeated and unwanted harassing behaviour by a person against another.
- Such behaviour may be reflected by a physical act or may be done through electronic means usually the internet and other communication devices.
- The act may cause mental trauma and fear to the victim, sometimes leading to more serious offences.
- The act is a direct intrusion into the privacy of an individual, where the stalker attempts to establish relationship with the victim without his/her consent.[103]

[99]B. Spitzberg and G. Hoobler, Cyberstalking and the Technologies of Interpersonal Terrorism, 4(1) NEW MEDIA & SOCIETY 71 (2002).
[100]BH Spitzberg and WR Cupach, The State of the Art of Stalking: Taking Stock of the Emerging Literature, 12 AGGRESSION AND VIOLENT BEHAVIOUR 64 (2007).
[101]D. Halder and K. Jaishankar, Cyber Crimes against Women in India: Problems, Perspectives and Solutions, 3(1) TMC ACAD. J. 48, 55 (2008).
[102]D. Lamplugh& P. Infield, Harmonising Anti-Stalking Laws, 34 Geo. Wash. Int'l L. Rev. 853 2002-2003.
[103]Dr.DebratiHalder, Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives, SSRN 103, 103-130 (2015)

Cyber Stalking is a serious form of harassment posing threat to life of an individual if it is not addressed appropriately. It constitutes harassment of individuals on cyber space through use of information and communications technology (especially the Internet). Such harassment may include actions such as the transmission of offensive and derogatory e-mail messages, identity theft and damage to data or equipment. As a result, cyber stalking is a set of behaviors in which a person, a group of individuals, or an organization uses information and communication technologies to threaten one or more people. Transmission of threats and false claims, identity fraud, data theft, data or equipment damage, computer surveillance, solicitation of minors for sexual purposes, and altercation are examples of such behaviors.

B. Cyber Stalking and Victimization of Women

It has often come to be seen that women and young children become victims of such acts leading to threat, harassment, assault and trauma. Privacy in virtual world as well as real life is gradually shrinking and women are the most affected community in this regard. Cyber Stalking is a serious example of infringement of privacy of women in cyberspace. In addition to this, because of the nature of the offence and the target aimed, such abnormal activities leave a serious impression on every aspect of their life.[104] Cyber victimisation of women can be categorised into two main groups: textual victimisation and graphical victimisation. Graphical victimisation may include producing, creating or publishing obscene, derogatory, and pornographic, including revenge pornographic materials on the web to put the victim in shame.[105]

There is no doubt about the fact that traditionally women are considered to be marginalized and disadvantaged section of the society. Even though the Constitution of India guarantees equal rights to men and women, women have been made second grade citizens due to dominantly patriarchal set up of the society. On many occasions, stalking becomes a vindictive instrument for man as an immediate reaction to refusal by the woman to get into any relationship with him. Today, the scenario is far more alarming where internet trolls take to social media website and instant messaging services like WhatsApp to target women activists, journalists, celebrities, academicians and so on to create hatred among the larger community against such women just to gain a sadist pleasure out of it.[106]

According to a comparative data of Working to Halt Online Abuse (WHOA) for the period 2000-2013, it was revealed that women victims generally outnumber male victims when it comes to cyber stalking victimisation and that out of 4043 victims who contacted WHOA in the said period, 70% were women. Women are targeted by trolls, bullies, stalkers with insulting, defamatory, derogatory statements/pictorial depiction on the internet. Even when women are not connected to the worldwide web, they may be harassed and stalked by unnecessary phone calls and SMSs. This may sometimes result in barring women completely from using any such medium of communication. This shows a blatant violation of rights of women through improper exercise of right to speech and expression on the internet. They are violation of basic human rights including right to equality as guaranteed under Article 14 of the Constitution of India as the right to live with dignity as enumerated in Article 21 of the

[104] John M. Deirmenjian, Stalking in Cyber Space, (1998)

[105] Dr.DebratiHalder, Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives, SSRN 103, 103-130 (2015)

[106] K. Y. A. McKenna, A. S. Green and M. E. J. Gleason, Relationship formation on the Internet: What's the big attraction?, 58 (1) J.OF SOCIAL ISSUES 9 (2002).

Constitution. Unfortunately, while deciding in the landmark case of Shreya Singhal v. Union of India, constitutionality of Section 66A of the IT Act, 2000, the Supreme Court emphasized on right to freedom of speech and expression, but overlooked the victimization of women in cyber space by misuse of this right. Such victimization would be dangerous for women because of the nature of electronic media which is different from print media.

4.4CYBER STALKING: LEGAL REMEDIES

Cyber stalking is a common phenomenon in cyberspace, which go unaddressed many a time due to lack of specific laws and enforcement mechanism. This is a glaring example of serious consequences of stalking in cyberspace. There could be end number of cases of similar nature which go unreported. Social norms and orthodox values play a major role here. Women victims and their family members feel reluctant to report such crime, especially due to fear of damage to their social reputation. Apart from this, there are various factual reasons for less number of prosecutions of cases of cyber stalking. This may include lack of focused laws, challenges in establishing identity of the perpetrator, lack of proper infrastructure in the criminal justice machinery in India and above all, the absence of servers within the jurisdiction of India, and conflict of laws between Indian laws and laws of countries which host the internet companies/service providers.[107]

The first initiative to formulate a legal framework for the cyber space was perceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India emerged in the form of the Information Technology Act, 2000 which was significantly amended in the year 2008. The IT Act also amended some of the provisions of the Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Though since 2000 the IT Act is in place in India for curbing offences like cyber stalking, the problem still remains unaddressed as the law is more on papers than on execution because lawyers, police officers, prosecutors and Judges are in a helpless state in apprehending its highly technical terminology.

The offence of cyber stalking was not incorporated in the IT Act when it came into force in 2000 unless the act involved publication or transmission of obscene material within the meaning of Section 67 of the IT Act. Besides, Section 509 of the Penal Code, 1860 (IPC) partially deals with the offence according to which uttering of any word, making of any sound or gesture or object to be heard or seen by a woman, or intrusion upon the privacy of such woman shall be punishable with imprisonment up to three years and fine. Since Section 509 of IPC defines this act as one of privacy, Section 72 of IT Act was used to deal with cases of cyber stalking to an extent. With the amendment of IT Act in 2008, Section 66A was inserted in the IT Act under which all the cases of cyber stalking were dealt with.

4.5 LET'S SUM UP

[107]Leroy McFarlane & Paul Bocij, Online Harassment: Towards a Definition of Cyber Stalking, 139 PRISON SERVICE .l 31, 31-38 (2002).

Cyber Stalking is a serious form of harassment on the internet. Besides, deciding on the jurisdiction for dealing with such offence is a challenge before the courts. Hence, there is a need for revisiting the IT Act for prosecution of cases of cyber stalking as well as law enforcement mechanism needs to be better equipped to address such problems in an effective manner. At the same time, the challenges involving law and technology in dealing with such offences must be addressed effectively to reduce the vulnerability of the users of cyberspace. The article puts forward the following suggestions and observations for a better redressal system for Cyber Stalking:

1. Global Crime: Need for International Cooperation The nature of most of the cyber-crimes is global in nature due to which the jurisdiction to investigate becomes a major issue. Whenever a stalking takes place in cyber space, the server of the electronic device used for such acts might be located beyond the territorial jurisdiction of India. Hence, it may be feasible to conduct investigation of such cases if it is made mandatory for the service providers such as Facebook, twitter or WhatsApp to install a local server in India. Such arrangement may, to some extent, be able to address the problem of jurisdiction in such cases.

2. Stringent laws at National Level In the absence of a specific provision to address cases of Cyber Stalking, it is highly essential to make necessary amendments in the existing laws or to bring Section 66A of the IT Act back with necessary regulations.

3. Need for Inter-State cooperation Due to serious lack of cooperation and coordination from another state involved in a crime, the investigating agency fails to complete investigation. In this regard, a Cyber-Crime Inter-State Cooperation Cell may be set up and attached with every cyber cell so that it provides exclusive information relating to such crimes.

4. Initiative at the Individual Level As a measure for protection from such exploitation in cyber space, it is necessary to take precautionary steps such as adequate security measures to ensure not to disclose personal information on the internet in inappropriate fora. Passwords should not be made too easy to be cracked by perpetrators. The privacy settings in social media facilitate blocking of accounts causing annoyance. The same must be taken recourse to avoid unnecessary harassment.

5. Revisiting the Right to Freedom of Speech and Expression: It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. There is a need for striking a balance between freedom of speech and expression on the one hand, and right to privacy on the other.

Cyber stalking has become a recent threat for the cyber community in India, especially women irrespective of age or any other social strata they belong to. It has even gone to the extent of ruining the lives of many young women. Therefore, it is the need of the hour to formulate a technically sound legal framework as well as an impartial mechanism for better redressal of cases of Cyber Stalking in India.

4.6FURTHER READING

- See Salem woman, 21, kills herself after obscene pictures morphed to look like her were posted on Facebook, Daily Mail, Jun. 29, 2016, available

at http://www.dailymail.co.uk/indiahome/article-3664841/Salem- woman-21-kills-obscene-pictures-morphed-look-like-posted-Facebook.html.

- DebaratiHalder& h. Jaishankar, Cyber Crimes Against Women in India 8 (2017).
- Ursula Smartt, The Stalking Phenomenon: Trends in European and International Stalking and Harassment Legislation, European Journal Of Crime, Criminal Law And Criminal Justice, Vol. 9/3, 209-232 (2001).

4.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the suggestions and observations for a better redressal system for Cyber Stalking?**

   Need for International Cooperation; Stringent laws at National Level; Need for Inter-State cooperation; Initiative at the Individual Level and Revisiting the Right to Freedom of Speech and Expression.

4.8 ACTIVITY

Elaborate the legal remedies available against cyber stalking. (1000-1500 words)

Block-4

CYBER TERRORISM

Unit 1: CYBER TERRORISM: AN ANALYSIS WITH AN INDIAN PERSPECTIVE

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Conventional vs. Cyber age terrorism

1.4 Forms of Cyber Terrorism

1.5 Judicial Response

1.6 Let's sum up

1.7 Further reading

1.8 Check your progress: Possible Answers

1.9 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Meaning of cyber terrorism in India
- Difference between terrorism and cyber terrorism
- Forms of cyber terrorism
- How judiciary has interpreted the cases of cyber terrorism

1.2 INTRODUCTION

Terrorism, as a part of the 21st Century, grew as a cult with an end in itself. Terrorism instils a fear in the minds of the people against their state's inability to protect them from damage in person and property; it also creates a psychological and social havoc in the lives of people. Conventional terrorism was aimed at eroding the tranquillity and tolerance among a group of people, or more precisely to disrupt the harmonious well-being of a nation.[108] With emerging trends in generations, terrorism has changed its shape and form, keeping pace with modern era. With the advent of the culture of the world being online, cyber-terrorism developed its roots to tackle the ever advanced techno-geek reality, forcing into the personal space of people without any visible damage. But is there any remarkable difference between conventional and contemporary forms of terrorism? What makes it different from cyber-attacks and renders it a form of terrorism? How does it affect the government and its policies? How does the law deal with it? While most of these are lethal, the question regarding their legality with respect to ethical hacking and security also arises.[109]

Cyber-terrorism has been defined by various organisations, adding various dimensions to its scope, but retaining the crux of the problem. NATO defines cyber-terrorism as "a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal." The National Infrastructure Protection Centre defines cyber-terrorism as, "a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction, and/or disruption of services to create fear by causing confusion and certainty within a given population conform to a political, social, or ideological agent." The most accepted notion of cyber-terrorism is defined by FBI which defines it as, "a premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." A close analysis of these definitions reveals some common aspects of cyber-terrorism which are inherently present in it - fear, political association and/or ideological influence. What can be gathered is a simple line-up for this term, i.e., Cyber-terrorism is a technologically transmitted

[108]S. Best, Defining Terrorism: http://www.drstevebest.org/Essays/Defi ning%20Terrorism.htm www.symantec.com/avcenter/reference/cyberterrorism.pdf

[109]M. Cereijo Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba. com/archivo/manuel-cereijo-110.htm

crime with intent to destroy or affect a set of information which is politically, morally or ideologically undesired by a group or race of people and to create a sense of fear so as to stop its future perpetuation. While cyber-terrorism is more or less assumed to be a form of hacking, the latter is subsumed by the former and thus encompasses a much wider centre-stage.[110]

1.3CONVENTIONAL VS. CYBER AGE TERRORISM

While most of the scholars believe that terrorism is a term which brings with it destruction, deaths, and devastation, the cyber-world of terror attacks is incapable of such level of desolation. The conventional mode uses more of physical warfare and weapons, including both men and matter, in order to gather more fear and pressure, and sometimes to give effect to their own macabre ideology. Scuttling of peace attains topmost ground in a terror instance. On the other hand, the 'cyber enabled terrorism' uses virtual mode to delve into the lives of people and disturb them psychologically and financially. It uses a more formal approach of maliciously transmitted viruses and ransom wares. The motive behind cyber-terrorism is usually not personal, and this is what differentiates it from cyber-crime. The end result of cyber-terrorism may include shut down of networks, money extortion for terrorism purposes, stealing of information, and hacking of government systems. Just like the recent instance of 'Wannacry' ransom ware that hit more than 150 countries and demanded payment of 'Bitcoins', another cyber-related terrorism.[111] The 'Flame' malware that hit the Middle-Eastern countries in 2012 is also an example of cyber-terrorism. Although, this form of terrorism is not as much devastating as its other counterpart, it is gaining more ground due to its other attributes, that is to say that it is comparatively easier to spread with no costs and no limits. Also, the identity of the perpetrator can be concealed along with his/her location. Cyber-terrorism has thus created a niche for itself with it being the 'new' normal.

1.4FORMS OF CYBER-TERRORISM

With the advancement in the technological world, the cyber related crimes are on an increase with every coming day and it is humanly impossible to attempt a categorisation of the same. Cyber-terrorism can acquire new dimensions, with an edge in almost every sphere and thus, the types of crimes are endless. While we await newer forms to dig up, the following forms are not hard to compile:

- **PRIVACY VIOLATION**

Every individual has a right to live in privacy and the right to be let alone. The Right to privacy gained recognition under Articles 21 and 19(1) (d) of the Indian Constitution in post-Maneka era. Also, privacy is an independent and distinguished concept recognised by the tort law, although it is not exercised much in

[110]R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation, Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee Washington, DC, 05 April 2001, http://www.fbi.gov/news/testimony/issue-of-intrusions-intogovernment-computer-networks
[111]R. Lemos, Cyberterrorism: The real risk, 2002: http://www.crime-research.org/library/Robert1.htm

India in that context. As 'Privacy' has now gained status of fundamental right, it is well protected by both civil and criminal consequences. With the dawn of solidarity-oriented culture, people have become more and more sensitive to the invasion of their personal space, not only physical but also mental. To cope up with this intrusion done by information technology, the legal society has evolved a fresh new outlook, although not so advanced. Privacy violation may include information access without the consent of the person or the organisation involved, or passing off of information by an agent to a person not authorised to do so. Cyber-terrorism invades the right to privacy of an individual. The acts of cyber-crime are a threat to personal information and activities of a person and can be treated as a form of cyber-terrorism. It may include phishing, hacking of accounts, transmission of viruses etc.[112]

- **DATA THEFT AND MISAPPROPRIATION**

Cyber-terrorism also aims at leaking out confidential information not only of private individuals but also of the government and other agencies. Such information may be of national importance and of vital nature with respect to the security and defence of a country. It can be used by terrorist outfits to facilitate their objectives and to further facilitate their infiltrations by finding the probable lacunae in the system. The same may be used to destroy property which is public or private, movable or immovable, and tangible or intangible. Data misappropriation is another tool of cyber-terrorism to tackle the odds. Data on a source can be manipulated to gain access to a particular object, while denying the same to the owner. This renders the security systems useless and puts information under seize.

- **DEMOLITION OF E-GOVERNANCE BASE**

The e-governance is the main source of interaction between state and its citizens. The right to information is also an outcome of the e-governance. While it facilitates transfer of information on one hand, it also helps in raising voices and opinions on particular policies and actions. The government acts as a custodian of public information, ranging from personal information of its citizens to data related to their public activities. The public has a right to information; however, it is not an absolute privilege to them. The Hon'ble Supreme Court of India in People's Union for Civil Liberties v. Union of India held that the government can withhold information related to various matters on certain grounds. While most of this information is in hard-copy form, the digital version is susceptible to a probable cyber-attack. Such an attack could cause a complete demolition of this established e-governance base.

- **DISTRIBUTED DENIAL OF SERVICE ATTACK**

Distributed Denial of Service (hereinafter DDoS) is a kind of attack where-in multiple 'infected' computer systems or servers attack another system or server, which causes the affected computer to 'deny' service to the user. The affected computer is actually flooded with endless data and information which causes the server to slow down or crash, which further causes it to stop working and denies the service requested or required by the legitimate user of the server. This works as an interlinked web of infections spreading from one system to another vulnerable

[112] A. Jahangiri, Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion: http://www.alijahangiri.org/publication/Cyberspace-Cyberterrorism-andInformation-Warfare-A-Perfect-Recipe-for-Confusion.htm

system and finally attacking a single targeted system. The purpose of using multiple systems to attack a single system is manifold; first, it becomes impossible to block all the infecting systems, and second that multiple systems transmit large amount of traffic, so the collapse of infected system is ensured. Such an attack causes a communication break between various heads and also leads to monetary losses. On a national level, a DDoS can cause system slowdown and hinder efficient administration by the government, while at the same time hovering as a constant threat to national security and integrity.[113]

1.5JUDICIAL RESPONSE

The Judiciary has a very important role to play when it comes to controlling the menace of cyber-terrorism. With the advent of judicial activism, or rather judicial adventurism, the Indian Judiciary has got a new dimension to venture into. The first issue which the Judiciary may face is of jurisdiction as before going into the merits, it should be satisfied that it has the requisite jurisdiction to do so. Since internet is not a 'single-entity owned or government operated', it cannot be regularised as an ordinary crime by invoking the jurisdiction. Again, the cross-border terrorism may also give rise to the problem of jurisdiction. The Indian Judiciary may have the jurisdiction to deal with these cases if the victim is in India, and/or the perpetrator is present in India, or the cause of action lies in India, or if the primary effect of the attack is on India. Another situation may arise when none of the given situations are present, but extraordinary circumstances are present and the country's sovereignty or security is at stake. In that case too, the Judiciary may have the jurisdiction to take up the matter. Otherwise also, section 1(2) read with section 75 of the Information Technology Act, 2000 gives courts the jurisdiction to deal with matters outside India. Apart from the jurisdictional matters, the Judiciary should also be well equipped with appropriate and adequate laws to decide the matters with utmost strictness and provide harsh and deterring punishments to the originators of these attacks. An active Judiciary must be backed with laws that are generic and living in nature, further watered by way of precedents. Lack of precedents causes hindrances in development of the law as without judicial interpretation, the law remains confined to its literal meaning and there is little scope to fill up the lacunae therein. The role of Judiciary must be supported by the whole lot of citizens and netizens who reap the benefits of internet but are targeted as victims. But at the same time, it is the duty of the court to ensure anonymity and security to them.

1.6 LET'S SUM UP

Efforts should be made to make a comprehensive law with both national and international approach to stop cross-border cyber-attacks with a smooth mechanism for redressal. Adopting a mutual code of cyber legislation can go a long way as cyber-terrorism knows no borders and thus, a well incorporated mechanism must be evolved. If internet can be used to spread terrorism, the same can be used to

[113]E. Waak, The Global Reach of Privacy Invasion, Humanist, November/December 2002: http://www.thehumanist.org/humanist/articles/waakND02.htm

tackle it also. The Ministry of Electronics and Information Technology, Government of India's 'e-security' scheme is a well applauded step in this direction. While there can be various approaches to deal with this issue, the one provided in the United Nations' Counter Terrorism Implementation Task Force seems to be the most rational and practical one. According to Counter-Terrorism Implementation Task Force (CTITF), working group of UN, this proposition should be approached by a multi-disciplinary approach, involving experts in counter-terrorism, technology, law, public policy, law enforcement and human rights. As a single agency cannot deal with this issue, in the same way, a single legislation may not serve the purpose. Cyber-terrorism control can be put onto other Acts as well. For instance, online frauds because of online transactions and contracts can also come under the ambit of the Indian Contract Act, 1872 and the Sale of Goods Act, 1930. Protection of intellectual property is also one of the major problems in this era, be it inventions, formulae, movies, books, ideas or recipes and so on and so forth. The Indian Copyright Act and the Indian Trademarks Act may be altered to invoke special attention to this issue with respect to cyber-terrorism. As far as other illegal activities on the internet are concerned, while the Information Technology Act penalises them, other legislations may govern them. A specific legislation for this purpose may solve the problem to an extent, but as the gamut of cyber-terrorism is expanding, a holistic legal development is required to tackle this issue effectively. This may demand amendments in the existing statutes, a lot more oriented research and development, combined with the ability of secure technology, an active government agency and an open-eyed Judiciary.

1.7FURTHER READING

- NIPC, 'Cyberterrorism : An Evolving Concept. National Infrastructure Protection Centre' (National Infrastructure Protection Centre, June 2015) <www.nipc.gov/%20NIPC>
- M Gercke, 'Understanding Cybercrime : A Guide for Developing Countries' (International Telecommunication Union, March 2011) <www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf>
- Urgent measures for combating international terrorism' (Decree-Law, 27 July 2005) <www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026>

1.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **How does cyber terrorism affect government agencies?**

   Cyber-terrorism also aims at leaking out confidential information not only of private individuals but also of the government and other agencies. Such information may be of national importance and of vital nature with respect to

the security and defence of a country. It can be used by terrorist outfits to facilitate their objectives and to further facilitate their infiltrations by finding the probable lacunae in the system. The same may be used to destroy property which is public or private, movable or immovable, and tangible or intangible.

1.9 ACTIVITY

Explain the judicial response towards the menace of cyber terrorism. (1000-1500 words)

Unit 2: THE CYBER TERRORISM CONUNDRUMAND 'PROTECTED' SYSTEMS

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Sections 70 & 66F of the IT Act: An Insight into the Concerns

2.4 Addressing The Concerns Regarding Section 70

2.5 Let's sum up

2.6 Further reading

2.7 Check your progress: Possible Answers

2.8 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Mens rea under the Information Technology Act, 2000
- The implications of sections 70 and 66 F of the IT Act, 2000
- The doctrine of mens rea under sections 70 and 66 F of IT Act, 2000

2.2 INTRODUCTION

"Crime is crime because it consists of misconduct that explicitly and seriously violates society's welfare or well-being, and that it is not safe to leave it redressable only by restitution of the person injured." After reading these lines, one can see how serious an act that constitutes fraud is: "wrongdoing that specifically threatens society." Equally important is the observation that it is something that cannot be remedied only by monetary rewards. However, there is something more important than the act (of wrongdoing) itself that this meaning ignores, including the accused's mens rea.[114] International criminal law recognizes that no offence, major or minor, may occur without an immoral mind, since the nature of a crime is its unlawful purpose, without which it cannot exist. As a result, punishing behavior without considering the actor's state of mind is both ineffective and unfair.

2.3SECTIONS 70 & 66F OF THE IT ACT: AN INSIGHT INTO THE CONCERNS

To begin, what exactly is a guilty mind? Since each offense consists of a prohibited act or omission together with whatever state of mind is required by the law that bans it, the answer to this question will vary. In this respect, the Penal Code of 1860 has numerous components relating to mens rea in phrases like "intentionally," "knowingly," "dishonestly," and so on. The Information Technology Act of 2000 (hereinafter "IT Act") also allows for such words.

However, the language of Section 70(3), which punishes simply gaining access to a protected system: "Any individual who secures or attempts to secure access to a protected system in contravention of the provisions...", contains no such requirement. Second, this issue leads to another, seemingly pointless question: should the legislature's purpose be to acquit an individual even though he has perpetrated the act with the intention "ordered" by the legislative provisions? This question would be resolved affirmatively under two circumstances: first, when the legal clause is not worded according to the legislature's purpose; and second, when the provision is not implemented according to the legislature's meaning. Both of these scenarios are crucial in the context of Section 66F of the IT Act. The statute is

[114]See: Gabriel Weimann, 'Cyberterrorism – How real is the threat', United States Institute of Peace, Special Report 119, December 2004; ZahriYunos and SharifuddinSulaman, 'Understanding Cyber Terrorism from Motivational Perspectives', *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), pp. 1-13; Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, Vol. 7, No. 11-4, November 2002.

divided into two parts: Section 66F (1) A and Section 66F (1) B of the IT Act, which specify the spectrum of cyber terrorism.

About the fact that it governs a serious crime like cyber bullying, the provision is too vague. The requirement of mens rea under the clause broadens the scope of the provision and causes concern in two respects. First, when we assume that an insecure system like the Aadhaar scheme falls beyond the scope of the provision, "knowingly" accessing a computer system without authorization becomes pretty straightforward to prove.[115] This is because the Aadhaar scheme is a framework that can only be lawfully obtained by a limited number of people. Furthermore, any leak of information from the Aadhaar database will be extremely harmful to the nation due to the current importance of such data. It would be easier to prove that the unauthorized access was followed by reasonable grounds to assume that the information was "likely to inflict harm to the sovereignty and dignity of India, the protection of the State,... public order."[116] As a result, the Aadhaar scheme can be inferred to be a device that is "limited for purposes of state protection" and hence comes under the purview of Section 66F (1) B of the IT Act. Second, someone who "knowingly" accesses any prohibited material or archive in regards to "contempt of court" or "defamation" falls under its purview. It should be remembered that slander or even contempt of court have little effect on state protection, making their presence impossible to explain. However, this Chapter is limited to the convenience of demonstrating entry to a computer device and does not address the inclusion of slander. The following section addresses the topic with the aid of an analogy.

A. AN ILLUSTRATION

The Unique Identification Authority of India (hereinafter "UIDAI" Aadhaar)'s scheme entails the gathering of biometric and demographic data from 1.3 billion individuals. It has created the world's largest biometric identity project, which must be carefully scrutinized to ensure that it complies with human rights. In reality, the database's wasteful management is not made available. Notably, the UIDAI has declared the Aadhaar database to be a "secure device" under Section 70 (1) of the IT Act, as well as stating that the biometric data stored is "important personal data" under Section 43A of the IT Act. The above section imposes on the UIDAI, which is a legal entity, an obligation of responsibility to enforce and uphold fair security standards and procedures. The Information Technology (Information Security Policies and Procedures for Protected Systems) Rules, 2018 (hereinafter "2018 Rules") outline the practices and procedures that must be followed in the case of protected systems (such as the Aadhaar database).According to the source, the UIDAI's compliance with most of the 2018 Rules' responsibilities is in doubt. This is as a result of the confirmed non-compliance. The 2018 Rules, for example, mandate that the UIDAI appoint a Chief Information Security Officer (hereinafter "CISO"). However, it has been stated with proof that the UIDAI currently lacks a CISO. As a result, the authority has been unable to keep the details intact, despite its best efforts. The author wants to emphasize that the Aadhaar database is only secured for its own sake, and that the UIDAI is not following fair protection procedures in order to fulfill its obligations under Section 43A of the IT Act. Let's take a look at a data leak scenario against this backdrop. After being able to enter the Aadhaar database, say

[115] Defense Intelligence Agency, 'Cyberterror.Prospects and Implications', pp. 10 and 9, respectively.

[116] JonalanBrickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *CTC Sentinel*, August 2012, Vol. 5, No. 8, p. 6.

"A," an information technology student, circulated a connection on WhatsApp, reporting the "mismanagement" in the Aadhaar database.[117]
According to the WhatsApp links exchanged, he quickly hacked the personal information of 1.3 billion Indian people and made it available there. The connection has now reached thousands of people as a result of the subsequent sharing. Legally, gaining access to a computer device may or may not be considered a crime. To be held criminally liable, the individuals involved must be able to form the necessary criminal motive to commit the offense. Ethical hackers who break into a computer system for the sole purpose of seeing how it works do so with no intention of committing a crime. As a result, someone who wants to reveal the Aadhaar system's fallacy in order to raise public awareness about such a serious issue is not committing a crime just by accessing the database. As a result, "A," the hacker who gained access to the database, should preferably be exempt from all cyber-crime provisions. Surprisingly, a literal reading of the clause would place "A" as well as those who opened the shared connection under the purview of Section 66F of the IT Act. These people not only lacked authorization, but also knowingly accessed the device. This translates to them doing something that meets the requirements of the provision. To bolster his case, the author now adds a twist in the above-mentioned example (hereinafter referred to as "the modification"). Let's pretend that the connection posted by "A" does not currently have access to the database and has just come to the public's attention as a result of "A's" publicity stunt.
In this case, simply opening the connection would be considered a "attempt" to gain access to the device, which is punishable under Section 70 of the IT Act. In certain situations, one must consider the legislature's intent: was it the legislature's intention to prosecute those who accessed the connection exchanged on WhatsApp for crimes as serious as cyber terrorism under Section 70 of the IT Act? That certainly wasn't the case. These people, on the other hand, "knowingly" accessed information that was shielded for the sake of the state's protection and sought to enter a protected structure. As a result, they will be responsible under Sections 66F and 70 of the IT Act, according to current regulatory interpretation.[118]
At the same time, the UIDAI will exclude prosecution under Section 43A of the IT Act because it has never given clarification on the security mechanism in place to protect citizens' "sensitive personal data." Since the UIDAI's compliance with the 2018 Rules is unknown due to a lack of required details on the UIDAI's website, this is the case. This is significant because, in the case of covered structures like the Aadhaar database, the 2018 Rules are the applicable norm. Furthermore, there is a growing fear that the UIDAI has not implemented appropriate security procedures as a result of reports of non-compliance with the duty to nominate a CISO. To answer the author's questions about mens rea, consider the maxim of proportionality, which states that sentences should be proportionate in magnitude to the seriousness of a defendant's criminal behavior.[119] Applying this theory to the example, thousands of people who opened the connection out of respect for their personal information will be criminally liable and fall into the category of crimes punishable by incarceration for up to ten years or even a lifetime. The UIDAI, on the other hand, which has violated

[117]Daniel Cohen, 'Cyber terrorism: Case studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13.
[118]Department of Justice, 'ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison', *Justice News*, September 26, 2016.
[119]Ellen Nakashima, 'U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election', *The Washington Post*, December 25, 2019

a severe duty to keep information confidential, is only liable for a civil wrong under Section 43A of the Act, which it avoids in any situation due to the provision of “fair” action.As a result, the statute’s wording ignores the concept of proportionality, which, like mens rea, is a foundational principle of criminal law. The same thing should be taken into account when drafting criminal laws. After determining the location of the problem, it’s a good idea to include some concepts and provisions that will help you come up with a solution.

2.4ADDRESSING THE CONCERNS REGARDING SECTION 70

Examining Section 66 of the IT Act’s general clause on “computer based crimes,” whereas Section 70 of the IT Act to further reflects the legislature’s purpose. Acts coming under Section 43 of the IT Act that are performed “fraudulently or dishonestly” are punishable under Section 66 of the IT Act, which is a penal clause. To put an act into the scope of Section 66 of the IT Act, two broad requirements must be met. First, the act must fall under the scope of Section 43, and second, the act must be performed with the intent to defraud or deceive. The act of accessing a computer, storing, copying, or removing any data or material from such a computer is covered by Section 43 of the IT Act in its particular portion. The investigation, on the other hand, has nothing to do with the first ingredient. It is important to emphasize the requisite intention for our purposes. In a nutshell, the two degrees of purpose listed in the provision are as follows:
When anything is done fraudulently, it is done with the intent to defraud. When the deceiver receives a reward or profit, or even the possibility of receiving a gain as a result of the deception, he is said to have an intention to “defraud.”
Dishonestly - A deceptive motive is that that seeks to achieve unfairly by obtaining something one does not have. Wrongfully gaining clearly refers to gaining illegally.
Let us use this legal matrix to see if the conduct of those who tried to enter the Aadhaar database by clicking on the connection met the legal requirements. Their conduct does not trick anybody, nor does it entail an advantage, or even the possibility of one. As a result, it does not qualify as a deceptive act. Similarly, their conduct is not unethical as they do not want to reap unfairly. As a result, while the acts of the citizens do not meet the requirements of the less serious crime punishable under Section 66 of the IT Act, they specifically meet the requirements of the more serious offence punishable under Section 70 of the IT Act. As a result, adding one of the two degrees of purpose included in the former section as an additional condition to the latter would limit the scope of the provision. As a result, situations like the one described above would fall beyond the scope of the clause, resolving the issue to a large degree.

2.5 LET’S SUM UP

This demonstrates how many criminal aspects of the IT Act, which were written in a broad sense, require more specific language to preclude ethical hackers. This necessity necessitates the inclusion of other degrees of mens rea in the provisions of Sections 66F and 70 of the IT Act. Alternatively, if an amendment requiring the use of mens rea as a component of the offence is deemed unsuitable, there is a remedy.

The issue of ethical hackers could be addressed by establishing a system of officially authorizing ethical hacking by legislation or subordinate legislation. This will, to a large degree, suffice in answering the author's questions. While the government, and in the event of its failure, the judiciary, must ensure that the UIDAI complies with the 2018 Rules, the suggested solutions for Sections 66F(1)(B) and 70 of the IT Act require legislative or executive action in the manner recommended in the preceding paragraphs. These provisions must be written in a way that represents the legislature's purpose while also facilitating their proper execution. The author acknowledges that the IT Act is a comparatively recent statute that is currently experiencing drastic revisions, but he addresses these topics that need to be addressed immediately.

2.6FURTHER READING

- Aadhaar in numbers: key figures from UIDAI CEO's presentation to the Supreme Court, THE HINDU, March 22, 2018.
- Editors' Guild, Others Condemn FIR Against Journo For Exposing Aadhaar Data Leak, Demand Centre's Intervention, LIVELAW.IN, January 7, 2018.

2.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What constitutes a guilty mind?**

   Various components related to mens rea are used in words such as "intentionally," "knowingly," "dishonestly," and so on, according to the Penal Code of 1860. The Information Technology Act of 2000 (hereinafter "IT Act") also allows for such words.

2.8 ACTIVITY

Explain the concerns associated with sections 77 and 66F of the IT Act. (1000-1500 words)

3

Unit 3: COUNTERING CYBER TERRORISM EFFECTIVELY

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Motivations for Cyber Terrorism

3.4 Types of Cyber Terrorism Attack

3.5 Psychological Effects of Cyber Terrorism to Humans

3.6 Let's sum up

3.7 Further reading

3.8 Check your progress: Possible Answers

3.9 Activity

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- How to counter cyber terrorism effectively
- Reasons for cyber terrorism
- Types of cyber terrorism attacks
- Mental effects of cyber terrorism

3.2 INTRODUCTION

The Federal Bureau of Investigation (FBI) and the System Administration, Networking, and Security Institute (SANS) released a list of the top 20 flaws in Internet-connected networks in 2001, according to a survey reported by PCWorld.com online magazine. The study advised companies to close the dangerous gaps in order to prevent potential cyber terrorist attacks. “The Internet is clearly not ready because of these vulnerabilities; we’re not ready to survive a massive attack,” says SANS Institute Director Allan Paller in the post.[120]

We can’t help but concur with Allan’s viewpoint on the subject. We will find it incredibly difficult to protect ourselves from cyber terrorist threats due to the massive and free existence of cyberspace. As a result, it is critical that we delve deeply into the problems of cyber terrorism and gain a thorough understanding of them in order to defend our nation’s, industries’, and personal interests from cyber attacks. Cyber terrorism is characterized as electronic attacks from cyberspace, originating from both internal and external networks, especially the Internet, that are directed at a specific target and originate from a variety of terrorist sources with varying motives.

Cyber terrorists typically see high-profile elements of a country’s sensitive infrastructures or company activities as their targets. The primary goal of these terrorists is to do significant physical and psychological harm to targets by doing damage that compromises or destroys them. “The ultimate threat to information security is the insider,” says Clifford A. Wilke. It is a well-known phenomenon that the majority of data breaches occur inside organisations. As a result, cyber terrorism may also take the form of computer assaults carried out by sanctioned insiders, through which the terrorists have gained internal access to networks and databases by different means, such as jobs with the organisation. Internal threats are much more risky than external attacks, owing to the obvious difficulty of identifying them. In addition to overt insider threats, unsafe relationships with contracting firms who recruit or have been compromised by attackers may be hazardous. As a result, it is critical that efforts to combat cyber terrorism begin at the source, which means that organisations must prioritize internal and external security equally, if not more than external security.[121]

[120]Thibodeau, Patrick. “Internet Vulnerabilities to Cyberterrorism Exposed. “ 1 October 2001. URL: http://www.pcworld.com/news/article/0,aid,64224,00.asp

[121]A. Wilke, Clifford. “Infrastructure Threats from Cyber-Terrorists.” 5 March 1999. URL: http://www.occ.treas.gov/ftp/bulletin/99-9.txt

3.3MOTIVATIONS FOR CYBER TERRORISM

Terrorists use cyber warfare as a means of inflicting harm or destruction to their targets for a variety of reasons.[122] Terrorism attacks have four key goals: disrupt enemy organizational capability, destroy or distort the prestige of an organisation, country, or alliance; force those targeted to change affiliation; and show to their own supporters that they are capable of causing serious harm on their objectives.[123]

- **To destroy enemy's operational capabilities**

  This is the primary justification for the use of cyber terrorism. Terrorists believe that using cyber capabilities provides them with a low-cost and reliable way to seriously harm or kill their targets, preventing them from continuing their regular operations. The results of such attacks, if effective, can be devastating in a variety of ways, including significant economic and social collapses. If vital infrastructure and company activities are disrupted, an entire country or business may be brought to a halt.

- **To destroy or misrepresent the reputation of an organization, nation or alliance**

  One of the key aims of cyber terrorism is to do this. Because of their unmistakable and solid prestige, many organisations, states, and associations are able to act successfully and are well valued and esteemed. If this critical component is tainted, it could have a significant effect on the targeted entity's daily operations. Web site defacements and circulating fake news about the target through electronic means such as e-mail, web pages, and others are the most common methods of undermining or misrepresenting the target's credibility.

- **To persuade those attacked to change affiliation**

  Cyber bullying is often used to compel attacked organisations to alter their relationship or association with specific groups. Despite the fact that achieving this objective is even more difficult, it has been accomplished in the past. To defend against such motivated threats, the attacked entity must form close relationships with its partner organizations in order to properly manage the situation or prevent it from occurring in the first place.[124]

- **To demonstrate to their own followers that they are capable of inflicting significant harm on their targets**

  Cyber militants are now eager to carry out cyber attacks in order to demonstrate to their fans and the rest of the world that they are capable of

[122]Sproles, Jimmy; Byars, Will. "Statistics on Cyber-terrorism." 1998. URL: http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm

[123]Axelrod, C. Warren. "Security Against Cyber Terrorism." 27 February 2002. URL: http://www.sia.com/iuc2002/pdf/axelrod.pdf.

[124]Erbschloe, Michael; Vacca, John. Information Warfare: How to Survive Cyber Attacks. Reading: McGraw-Hill Osborne Media, 2001.

wreaking havoc on their targets. There are so many people who are sceptical of the realities of cyber terrorism and its capability. As a result, if cyber criminals feel compelled to demonstrate their ability to carry out electronic-based attacks on their targets, they will do so to demonstrate their "prowess" to the rest of the world.[125]

3.4TYPES OF CYBER TERRORISM ATTACK

Cyber threats use a number of different forms of cyber warfare attacks. Cyber terrorism capabilities can be classified into three groups, according to the Naval Postgraduate School in Monterey, California's Center for the Study of Terrorism and Irregular Warfare: "simple-unstructured," "advanced-structured," and "complex-coordinated."

- **Simple-Unstructured**

  The ability to use software developed by others to perform simple hacks on specific systems. This style of enterprise has restricted target analysis, command, and control skills, as well as learning capabilities.
- **Advanced-Structured**

  The ability to launch more complex attacks against different devices or networks, as well as the ability to change or build simple hacking techniques. The company has basic goal analysis and command and control abilities, as well as a limited learning capacity.
- **Complex-Coordinated**

  The ability to launch concerted assaults against interconnected and heterogeneous defenses in order to cause widespread destruction. Terrorists are capable of using advanced hacking techniques. They may also perform target analysis and command and control operations. They still have a high level of organizational learning capabilities.

Incursion, disruption, misinformation, denial of service, and defacement of websites are the five major forms of cyber crime attacks. Some of these attacks are more serious than most, and they both have different goals. It is important that we consider the multiple attack tactics in order to achieve a greater understanding of how they can be successfully countered.[126]

- **Incursion**

  These attacks are carried out with the aim of obtaining access to or breaching computer systems and networks in order to obtain or alter data. This is a common and commonly used approach with a high success rate. Terrorists can exploit several loopholes in vulnerable operating systems and networks to

[125]Glaessner, Thomas; Kellermann Tom; McNevin, Valerie."Electronic Security: Risk Mitigation In Financial Transactions". June 2002. URL: http://www1.worldbank.org/finance/assets/images/E-securityRisk_Mitigation_In_Financial_Transactions-3.0.pdf

[126]Bryen, Stephen. ITU Workshop on Creating Trust in Critical Networks Infrastructure."A Global Security Approach to Protecting the Global Critical Infrastructure." 2002. URL: http://www.itu.int/osg/spu/ni/security/workshop/ presentations/cni.20.pdf

access and/or change sensitive information that can be used to do more harm to the organisation or for personal benefit.

- **Destruction**

  This kind of intrusion is used to break into computer systems and networks with the purpose of causing significant harm or damaging them. Depending on the nature of the attacks, the effects of such an incident can be devastating, with organisations being forced to shut down for an indefinite period of time. It will be very expensive for impacted companies to have their activities back up and running, which would have a significant financial effect as well as a negative impact on their image.

- **Disinformation**

  This approach is used to disseminate rumors or facts that may have a significant effect on a specific goal. Whether or not the rumours are real, the use of such threats carelessly will cause uncontrollable confusion in a country or organisation. This method of attack is difficult to stop since it can be carried out in a matter of seconds without requiring access to the victim's computer or network systems.

- **Denial of Service**

  Denial of Service (or DOS) attacks, as they are more commonly called, are another popular attack type. E-commerce powered businesses that offer goods or services online are the hardest hit by such attacks. Cyber hackers have also been known to threaten public websites with this form of attack. DOS attacks are designed to bypass or interrupt online operations by overwhelming targeted servers with a large number of packets (requests), causing the servers to become incapable of handling regular service requests from legitimate users.The consequences of such attacks can be devastating from both an economic and social standpoint, resulting in significant casualties for organizations.

- **Defacement of web sites**

  This method of assault is designed to deface the victims' websites. The websites may be completely redesigned to include messages from cyber criminals for marketing or advertising reasons, which may result in their removal, or they can be redirected to other websites that may include identical messages. Since more people are aware of the issue, the frequency of such attacks has decreased in recent years. However, a limited number of such incidents continue to occur, necessitating the implementation of appropriate monitoring protocols in order to prevent such humiliating and financially disastrous circumstances from occurring again.[127]

3.5PSYCHOLOGICAL EFFECTS OF CYBER TERRORISM TO HUMANS

[127]Shahar, Yael. "Information Warfare: The Perfect Terrorist Weapon." 31 October 2001. URL: http://www.ict.org.il/articles/infowar.htm

It goes without saying that if cyber terrorists destroy or threaten the nation's vital infrastructures or business processes, the people who are personally impacted will experience immense psychological trauma. We must not underestimate the psychological effect of cyber terrorist threats, when various individuals respond differently to certain circumstances. Any individuals that are personally impacted by cyber attacks, such as those that lose sensitive business information that can be used to endanger the organization's or the targeted person's well-being, can become fearful and live under extreme stress.
The person(s) affected may be physically harmed, which can have an effect on his or her mental health. In other situations, where misinformation attacks are carried out using blogs, e-mail, and other electronic means to refute rumors about a specific circumstance, organisation, or individual, the general public can experience chaos. People would panic, causing daily company practices and lifestyles to be affected. As a result, it is critical that the general public is well-informed about cyber terrorism and is able to recognise the actions that can be done to help address the issue. Psychological topics relating to the impact of cyber warfare on individuals, as well as appropriate approaches to treat related disorders, can be addressed more often in order to offer a reliable and better avenue for people who are concerned about those issues.

3.6 LET'S SUM UP

And if most of us are new to the world of cyber crime, it has proven to be a difficult one. In several nations, substantial progress has been made in protecting against cyber attacks thanks to business and government programs. It is universally acknowledged and understood by all that defense is not a one-stop shop. Instead, it's a never-ending path that everyone involved must be dedicated to. Understanding the various motivations and forms of threats, as well as considering the impact of cyber crime on sensitive infrastructures, enterprises, and individuals, as well as taking the often complex measures to reduce the chances of such attacks occurring, makes the challenge of defending against it such an enviable one. However, strategic security initiatives and strengthened working relationships among different bodies, including industry, government, and the general public, give us all a good chance of winning this war. The truth is that cyber bullying is here to remain, and we still have a long way to go in successfully defending the nation's, corporations', and our interests. The good news is that, thanks to the numerous strategic strategies in progress, we are moving closer to our key goal of having a highly stable and efficient working climate.

3.7FURTHER READING

- Thibodeau, Patrick. "Internet Vulnerabilities to Cyberterrorism Exposed."
- A. Wilke, Clifford. "Infrastructure Threats from Cyber-Terrorists."
- E. Denning, Dorothy. Testimony before the Special Oversight Panel on Committee on Armed Services US House of Representatives "Cyber terrorism."

3.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the main factors of motivation for cyber terrorism?**

   Terrorism attacks have four key goals: disrupt enemy organizational capability, destroy or distort the prestige of an organisation, country, or alliance; force those targeted to change affiliation; and show to their own supporters that they are capable of causing serious harm on their objectives.

3.9 ACTIVITY

Explain the psychological effects of cyber terrorism on Humans. (1000-1500 words)

Unit 4: ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR AND OTHER CYBER THREATS

4

4.1 Learning Objectives

4.2 Introduction

4.3 “Routine” Failure v. Cyber Attack

4.4 Hacking and Terror

4.5 Cyber Crime and Economy

4.6 Let’s sum up

4.7 Further reading

4.8 Check your progress: Possible Answers

4.9 Activity

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The differences between the intelligence failure and cyber attacks
- The concepts of hacking and terror
- Impact of cyber crime on economy

4.2 INTRODUCTION

Cyber-terrorism is not the first time a new technology has been seized upon as creating a strategic vulnerability. While the match between theories of cyber-warfare and air power is not precise, a comparison of the two is useful. In reaction to the First World War, European strategists like Douhet and Trenchard argued that aerial bombing attacks against critical infrastructure well behind the front lines would disrupt and cripple an enemies' capacity to wage war.[128] Their theories were put to the test by the U.S. Army and Royal Air Forces during World War II in strategic bombing campaigns aimed at destroying electrical power, transportation and manufacturing facilities. Much of the first tranche of literature on cyber attacks resembles in many ways (and owes an unspoken debt to) the early literature on strategic bombing.

A key document for understanding how attacks on infrastructure affect societies is the Strategic Bombing Survey conducted by the United State during and after World War II. During the war, Britain and America launched thousands of heavy bombers that dropped millions of tons of high explosives on Germany, seeking to cripple its infrastructure, destroy its industrial base and break the will of the population to continue the war. Early theorists of air warfare had predicted that such an onslaught would paralyze or cripple the target.[129] What the survey found, however, is that industrial societies are impressively resilient. Industrial production actually increased for two years under the bombing and it was not until ground forces occupied Germany that resistance ceased: As the air offensive gained in tempo, the Germans were unable to prevent the decline and eventual collapse of their economy. Nevertheless, the recuperative and defensive powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations. Germany resorted to almost every means an ingenious people could devise to avoid the attacks upon her economy and to minimize their effect. The mental reaction of the German people to air attack is significant. Under ruthless Nazi control, they showed surprising resistance to the terror andhardships of repeated air attack, to the destruction of their homes and belongings, and to the conditions under which they were reduced to live. Their morale, their belief in ultimate victory or satisfactory compromise, and their

[128]Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002

[129]DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5, pp. 78–85,http://www.awwa.org/Communications/journal/Archives/J501es3.htm, see also Scott Berinato, "Debunking the Threat to Water Utilities," CIO Magazine, March 15, 2002,

confidence in their leaders declined, but they continued to work efficiently as long as the physical means of production remained. The U.S. found similar results from aerial bombardment during the Vietnam War.
Counter-intuitively, the effect of aerial attack was often to harden and increase popular support for continued resistance. The advent of nuclear weapons (and perhaps large precision-guided munitions) gave air power the ability to disrupt civil infrastructures needed to achieve the visions of Douhet, Trenchard or Mitchell, but cyber attacks do not pose the same level of lethality. One of the Strategic Bombing Survey's conclusions was that "The German experience showed that, whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary." However, cyber attacks are likely to be single attacks. Once a hacker has gained access and the damage done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line. Cyber attackers would continually need to exploit new vulnerabilities and new tactics to ensure sustained disruption. Cyber attacks also seldom if ever produce physical damage that requires time-consuming repairs.[130]

4.3"Routine" Failure v. Cyber Attack

Critical infrastructure protection creates a new set of problems for national security. Different actors are involved. The focus is on civilian and commercial systems and services. Military force is less important. The scope of these new problems depends on how we define national security and how we set thresholds for acceptable damage. From a legal or public safety perspective, no country will accept even a single attack on infrastructure or interruption of services.[131] If the goal is to prevent cyber-attacks from costing a single day of electric power or water service, we have set a very high standard for security. However, from a strategic military perspective, attacks that do not degrade national capabilities are not significant. From this perspective, if a cyber-attack does not cause damage that rises above the threshold of the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security.
It is particularly important to consider that in the larger context of economic activity, water system failures, power outages, air traffic disruptions and other cyber-terror scenarios are routine events that do not affect national security. On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine occurrence at the system or regional level, with service denied to customers for hours or days. Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect. For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers, terrorist groups or nation states (particularly for nation states, where the risk of discovery of what would be universally seen as an act of war far outweigh the limited advantages gained from cyber-attacks on infrastructure).

[130]Larissa Paul, "When Cyber Hacktivism Meets Cyber terrorism," SANS Institute, February 19, 2001 "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"
[131]Riptech Internet Security Threat Report, July 2002

4.4HACKING AND TERROR

Much of the early work on the 'cyber threat' depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other's websites. No critical infrastructures have been shut down by cyber attacks. Terrorists seek to make a political statement and to inflict psychological and physical damage on their targets. If terrorism is an act of violence to achieve political objects, how useful will terrorists find an economic weapon whose effects are gradual and cumulative? One of Al Qaeda's training manuals, "Military Studies in the Jihad Against the Tyrants" notes that explosives are the preferred weapon of terrorist because "explosives strike the enemy with sheer terror and fright." Explosions are dramatic, strike fear into the hearts of opponents and do lasting damage. Cyber attacks would not have the same dramatic and political effect that terrorists seek.[132]

A cyber attack, which might not even be noticed by its victims, or attributed to routine delays or outages, will not be their preferred weapon. If terrorism is an act of violence to create shock and achieve political objects, how useful will terrorists find an economic tool whose effects are at best gradual and cumulative? An analysis of the risk of cyber terrorism is also complicated by the tendency to initially attribute cyber events to military or terrorist efforts when their actual source is civilian recreational hackers. When DOD computer networks were penetrated in an attack that occurred in the late 1990s, the U.S. was quick to suspect potential opponents, particularly Iraq or China, as the culprit. U.S. officials debated the merits of an active defense and whether this was an act of war, justifying a counter-attack. As tension mounted, the U.S. discovered that far from being a hostile power, the source of the attack was two high school students in southern California. It is difficult, especially in the early stages of an incident, to determine if the attacker is a, terrorist, group, foreign state, criminals, or a teenager in California. However, a quick survey of incidents over the last four years suggests that criminals and bored teenagers are the most likely sources of attack. To this day, the vast majority of hacking incidents result from the actions of recreational hackers. While the press has reported that government officials are concerned over Al Qaeda plans to use the Internet to wage cyber-terrorism, these stories often recycle the same hypothetical scenarios previously attributed to foreign governments' cyber-warfare efforts.

The risk remains hypothetical but the antagonist has changed from hostile states to groups like Al Qaeda. The only new element attributed to Al Qaeda is that the group might use cyber attacks to disrupt emergency services in order to reinforce and multiply the effect of a physical attack. If cyber-attacks were feasible, the greatest risk they might pose to national security is as corollaries to more traditional modes of

[132]www.terror.net: How Modern Terrorism Uses the Internet, by Gabriel Weimann (Special Report 116, February 2004

attacks. Espionage opportunities created by a greater reliance on internet-accessible computer networks will create greater risk for national security than cyber attacks. Terrorist groups are likely to use the Internet to collect information on potential targets, and intelligence services can not only benefit from information openly available on the web but, more importantly, can benefit from the ability to clandestinely penetrate computer networks and collect information that is not publicly available. This is very different from hacking, in that in the event of a successful penetration of a hostile network, a terrorist group or an intelligence service will want to be as unobtrusive as possible.

A sophisticated opponent might hack into a system and sit there, collecting intelligence and working to remain unnoticed. It will not disrupt essential services or leave embarrassing messages on websites, but remain quietly in the background collecting information. Collection techniques for the Internet differ significantly from earlier signals and communications intercept techniques, and while different kinds of data will be collected, the overall effect may be to make some espionage activities much more rewarding. This topic, the implications for espionage of the greater use of computer networks and Internet protocols, deserves further study.[133]

4.5CYBER CRIME AND ECONOMY

Cyber attacks do pose a very real risk in their potential for crime and for imposing economic costs far out of proportion to the price of launching the attack. Hurricane Andrew, the most expensive natural disaster in U.S. history, caused $25 billion dollars in damage and the average annual cost from tornadoes, hurricanes, and flood damage in the U.S. is estimated to be $11 billion. In contrast, the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. Putting aside for the moment the question of how the estimates of the Love Bug's cost were calculated (these figures are probably over-estimates), the ability of a single university student in the Philippines to produce this level of damage using inexpensive equipment shows the potential risk from cybercrime to the global economy. The financial costs to economies from cyber attack include the loss of intellectual property, financial fraud, damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc.) make up a large proportion of the reported cost of cyber attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. For example, if a Distributed Denial of Service attack prevents customers from reaching one online bookseller, they may instead go to another to purchase their books. The aggregate national sale of books could remain the same although the first bookseller's market share would decline.[134]

A small number of customers may choose not to bother going to another site if their first choice is unavailable, but some of these lost sales may well be recouped by later return to the sight by the customer. Businesses face greater damage from financial fraud and theft of intellectual property over the Internet, crimes that continue to grow in number. Emphasizing the transnational nature of cyber security issues, the last few years have seen the emergence of highly sophisticated criminal gangs capable of exploiting vulnerabilities in business networks. Their aim is not terror, but

[133]The Diplomacy of Counterterrorism: Lessons Learned, Ignored, and Disputed (Special Report 80, January 2002

[134]For terrorism and counterterrorism links, visit www.usip.org/library/topics/terrorism.html

fraud or the collection of economically valuable information. Theft of proprietary information remains the source of the most serious losses, according to surveys of large corporations and computer crime. These crimes must be differentiated from the denial of service attacks and the launching of viruses. Denial of services or viruses, while potentially damaging to business operations, do not pose the same level of risk.

Cybercrime is a serious and growing threat, but the risk to a nation-state in deploying cyber-weapons against a potential opponent's economy are probably too great for any country to contemplate these measures. For example, writers in some of China's military journals speculated that cyber attacks could disable American financial markets. The dilemma for this kind of attack is that China is as dependent on the same financial markets as the United States, and could suffer even more from disruption. With other critical infrastructures, the amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery for a nation state could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda. Cyber attacks could potentially be a useful tool (albeit not a fatal or determinative tool) for non- state actors who reject the global market economy.

4.6 LET'S SUM UP

The Internet is a new thing, and new things can appear more frightening than they really are. Much of the early analysis of cyber-threats and cyber security appears to have "The Sky is Falling" as its theme. The sky is not falling, and cyber weapons seem to be of limited value in attacking national power or intimidating citizens. The examples presented in this paper suggest that nations are more robust and resilient than the early theories of cyber terror assumed. To understand the vulnerability of critical infrastructures to cyber attack, we would need for each target infrastructure a much more detailed assessment of redundancy, normal rates of failure and response, the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. This initial assessment suggests that infrastructures in large industrial countries are resistant to cyber attack. Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber- terrorism and cyber-warfare give them credit for, and cyber attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring service than early analysts realized. Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cybercrime may be not be fully appreciated by many observers.

This is not a static situation, and the vulnerability of critical infrastructure to cyber attack could change if three things occur. Vulnerability could increase as societies move to a ubiquitous computing environment when more daily activities have become automated and rely on remote computer networks. The second is that vulnerability could increase as more industrial and infrastructure applications, especially those used for SCADA (Supervisory Control and Data Acquisition), move from relying on dedicated, proprietary networks to using the Internet and Internet protocols for their operations. This move to greater reliance on networks seems

guaranteed given the cost advantage of Internet communications protocols (Transmission Control Protocol/Internet Protocol), but it also creates new avenues of access. These changes will lead to increased vulnerabilities if countries do not balance the move to become more networked and more dependent on Internet protocols with efforts to improve network security, make law enforcement more effective, and ensure that critical infrastructures are robust and resilient. From a broader security perspective, nations now face a range of amorphous threats to their safety that are difficult for the traditional tools of national security to reach. The lines between domestic and foreign, private and public, or police and military are blurring, and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.

4.7FURTHER READING

- U.S. Strategic Bombing Survey, Summary Report (European War), 1945.
- Barton Gellman, " Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2002
- DeNileon, Guy, "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2001, Volume 93, No. 5.

4.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is the difference between routine failure and cyber attack?**

   On a national level, where dozens or even hundreds of different systems provide critical infrastructure services, failure is a routine occurrence at the system or regional level, with service denied to customers for hours or days. Cyber-terrorists would need to attack multiple targets simultaneously for long periods of time to create terror, achieve strategic goals or to have any noticeable effect.

4.9 ACTIVITY

Explain the effect of cyber attack on economy. (1000-1500 words)

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in

BAOU
Education for All

Dr. Babasaheb Ambedkar Open University

(Established by Government of Gujarat)

PGDCL-204
Emerging Issues of Cyberspace

Post Graduate Diploma in

Cyber Law

(PGDCL)

2021

Emerging Issues of Cyber Space

Dr. Babasaheb Ambedkar Open University

Emerging Issues of Cyber Space

Course Writer

Dr Peter Ladis	Faculty of Law, Chankaya National Law University, Patna, Bihar
Dr DeeshaKhaire	Faculty of Law, Gujarat National Law University, Gandhinagar
Ms PrabhavatiBaskey	Faculty of Law, Gujarat National Law University, Gandhinagar

Content Reviewer

Mr Kumar Gurav	Faculty of Law, Chankaya National Law University, Patna, Bihar

Content Editor

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

Copyright © Dr. Babasaheb Ambedkar Open University – Ahmedabad. 2021

ISBN:

Printed and published by: Dr.Babasaheb Ambedkar Open University, Ahmedabad

While all efforts have been made by editors to check accuracy of the content, the representation of facts, principles, descriptions and methods are that of the respective module writers. Views expressed in the publication are that of the authors, and do not necessarily reflect the views of Dr. Babasaheb Ambedkar Open University. All products and services mentioned are owned by their respective copyrights holders, and mere presentation in the publication does not mean endorsement by Dr. Babasaheb Ambedkar Open University. Every effort has been made to acknowledge and attribute all sources of information used in preparation of this learning material. Readers are requested to kindly notify missing attribution, if any.

Dr.Babasaheb Ambedkar Open University

PGDCL-204

Emerging Issues of Cyberspace

Block-1: Introduction to Emerging Issues under Cyber Law

UNIT-1
A Study On Emerging Issues On Cyber Law 05

UNIT-2
Emerging Trends In Cyber Crimes In India: An Overview 15

UNIT-3
Study Of Latest Emerging Trends On Cyber Security And Its Challenges To Society 24

UNIT-4
Challenges To Enforcement Of Cyber-Crimes Laws And Policy **33**

Block-2: Artificial Intelligence and Cyber Law

UNIT-1
The Role Of Artificial Intelligence In Cyber Security 43

UNIT-2
Artificial Intelligence And Cyber Security: Opportunities And Challenges 54

UNIT-3
Artificial Intelligence Policy In India: A Framework For Engaging The Limits Of Data-Driven Decision-Making 63

UNIT-4
Prospects of Artificial Intelligence In Tackling Cyber Crimes 70

Block-3: Data Protection And Privacy

UNIT-1
AI And Privacy Law 81

UNIT-2
Data Protection And Privacy Protection On Public Cloud 88

UNIT-3
Privacy Issues And Data Protection In Big Data 95

UNIT-4
Privacy And Data Protection Laws In India 102

Block-4: International Law On Digital Rights

UNIT-1
Good Cyber Governance 110

UNIT-2
Privacy And Data Protection: An International Perspective 117

UNIT-3
European Data Privacy Law Developments 125

UNIT-4
Regulatory Policy On Data Protection 132

Block-1

INTRODUCTION TO EMERGING ISSUES UNDER CYBER LAW

Unit 1: A STUDY ON EMERGING ISSUES ON CYBER LAW

1

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Literature survey

1.4 Cyber laws

1.5 Various issues under cyber law enforcement

1.6 Future Scope

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible Answers

1.10 Activity

1.1 LEARNING OBJECTIVES

In this chapter we will learn-

- The challenges under cyberspace and the urgent need for reformation in India's cyber edict framework and various issues in which cyber law enforcement lacks.
- Provisions governing cybercrime in India.
- Suggestive measures to deal with cyber law.

1.2INTRODUCTION

In the scenario of technological development, around the world, it is rapidly growing in a very positive way. But along with that few anti things also comes to the limelight. One of the aspects is rapid growth of digital and network technology, which helped in developing a virtual world of cyberspace. Cyber space brings great boomin every field of lifestyle and economy but parallel to the same, there is a growth of new crime, which is called cybercrime. The internet was originally designed as a medium for science and knowledge exchange, but it is now used by both the victim and the perpetrator to conduct cybercrime. Communication, ecommerce, and e-governance became more transactional as time went by. Cyber rules cover all compliance questions pertaining to internet violence. As the number of Cybercrime such as unauthorized access and hacking, Trojan attack, virus and worm attack, denial of service attacks etc. are increasing; the need for related laws and their application has also gathered great force. Cybercrime has neither the origin, nor the reference in the law.[1] On the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to cyber space, cybercrime was divided into two categories and defined thus:

(a) Cybercrime in a narrow sense that is computer crime in which any illegal behaviour done by the means of electronic operations that targets the security of computer systems and the data processed.

(b) Cybercrime in a broader sense which is computer related crime any illegal behaviour committed by means of an operating system or network, including such

[1]ManeeshTaneja and Dr. D.B Tiwari," Cyber Law", International Referred Research Journal, vol.11 (21) October, 2010, pp. 63-65.

crimes as illegal possession or distributing information by means of a computer system or network.

According to the tactical aspect attacks to digital networks for the purpose of seizing control or even destroying infrastructures that are vital to governments and sectors are of the crucial importance. According to the Norton report frequency of cyber attacks on Indian assets, with the government and private infrastructure equally exaggerated. In July 2013 government published national cyber security policy and just after that it was reported that government official's emails had been hacked. The NCSP is far from answering all nuances of the cyber threat. It doesn't maximize its potential for optimum benefit it just only provides guidelines for the standard operating procedure. The crucial point of security concern related to telecom industry which is fully integrated into cyberspace is missing.[2]

In this a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers.

1.3LITERATURE SURVEY

The advancement in technology has resulted in an increase in illegal activity, and the IT Act of 2000 establishes procedures for dealing with cybercrime. This model has some advantages in terms of e-commerce, but it does not fix any of the challenges and issues immediately.[3]

The IT Act is regarded as a hazy statute since the scope of regulation in the sense of the internet is vague. Computer forensics is gaining importance in the field of cybercrime evidence investigation because, while evidence is tangible in the real world, it is difficult to expunge information from a computer system in the virtual world of cyberspace. To handle this, computer forensics requires an efficient and knowledgeable computer expert because any carelessness leads to the loss of evidence.

About the fact that the IT (Amendment) Act 2008 addresses further issues, the IPC does not use the word "cybercrime" at any time. Since the year 2008, there has been a surge in cybercrime as hackers find loopholes in the legislation and use them to

[2]Yougal Joshi and Ananda Singh, "A Study of Cyber Crime and Security Scenario",International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18.

[3]Ravikumar S. Patel and Dr.DhavalKathiriya, "Evolution of Cybercrimes in India" International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.

carry out illicit activities. Cybercrime may be used to harm people, goods, or the government. There are few court precedents to refer to, and old statutes didn't always suit the offense at hand. There is a pressing need to enforce cyber rules. Our scheme can have harsh penalties to serve as a barrier to any illegal activities.

The IT Act (amendment) of 2008 broadened the scope of cyber law. The meaning section of the Proof Act has been changed. The problem of territorial sovereignty is a big one that the IT Act of 2000 does not adequately resolve. It is commonly observed that investigators stop taking cases on the basis of jurisdiction.[4] India's development has not been realized in all aspects, including E-courts, online dispute resolution, good cyber law, cyber forensics, and so on. The Information Technology Act has to be updated. In addition, science and academic professional preparation for lawyers should be made available in India.

Cybercrime is a new form in crime that has the potential to destroy any area of life because it is simple to commit but extremely difficult to find and trace in terms of jurisdiction, considering the geographical indeterminacy of the internet.[5]

To protect the emerging ICT, Cyber Security is needed. The advisory group should identify and suggest a good combination of options for vital ICT structures that complement the nation's governance framework. Understanding the cyber challenge and improving offensive capabilities in this cyber environment is a must. Nations, non-state entities, jihadists, organisations, and individuals are all posing a threat to development, which is becoming increasingly reliant on the cyber domain, necessitating the identification of technologies in this region.[6]

An adversary is an individual who commits a malicious act. Outsiders and insiders will also be adversaries. Insiders are not the same as outsiders. An insider is a person who has been granted access to a nuclear reactor or other classified operations. They were praised for their legitimacy, which included the ability to win admission. Cybercrime is a multibillion-dollar epidemic, and in order to realize the full potential of the computer era, appropriate legislation is needed to prevent overshadowing.

Governments and businesses all over the world are concerned with cyber security. Cyber-threats can take the form of cyber-attacks, but they can also occur as a result

[4]Talwant Singh, "Cyber Law and IT" pp. 1-4
[5]Rohitk.Gupta, "An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective", 2013.
[6]Rohit k Gupta, "An Overview of Cyber law vs. Cybercrimes", 2013.

of “mistakes” or natural disasters. As a result, in the context of cyber security, a specific solution to the specific problem is needed. In cyberspace, there are many problems to be discussed, including data security legal issues, a plethora of spans, cloud infrastructure legal issues, mobile law challenges, and social media legal issues. To keep fraudsters at bay, the builders must go beyond and beyond, and this should be the responsibility of three parties: (1) the king, authorities, and lawmakers; (2) the internet and network service provider or bank; and (3) the internet and network service provider or bank. (3) the individual, in their respective roles, to be responsible for information security.[7]

1.4CYBER LAWS

The 20th century introduced new requisites and offenses to the law glossary. Legal provisions should provide assertion to users, enforcement agencies and deterrence to criminals as it is very important to understand that computer cannot commit a crime but act of people. It is the human beings, not machines, who abuse, demolish and distort information. By realizing the need to combat with the cyber violations, the UNCITRAL, i.e. the United Nations Commission on International Trade Law adopted the Model Law of Electronic Commerce in 1996.[8] It was followed by the General Assembly of United Nation’s recommending that all states should give favourable considerations to the State Model law. In discharge of its responsibility, Government of India also accepted the need to legislate and has approach with the new legislation Information Technology Act, 2000. It was amplified by its amendments. The major acts, which got amended after enactment Information Technology Act, are Indian Penal Code (e.g. 192, 204 ,463, 464, 468 to 470, 471, 474, 476 etc) prior to enactment of IT Act, all evidences in a court were in the physical form only after existence of IT Act, the electronic records and documents were recognized. The Act essentially deals with the following issues:

- Legal identification of Electronic document.
- Legal identification of Digital Signatures

[7]PrabhatDalei and TannyaBrahme, “Cyber Crime and Cyber law in India: An Analysis”‘International journal of humanities and Applied science’ Vol.2 (4), 2014.
[8]Aashish Kumar Purohit, “ Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, vol.2(5) sepoct, 2011.

- Offenses and Contraventions Justice
- Dispensation Systems for cybercrimes.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes as from the prospective of E-Commerce in India, IT act 2000 contains many positive aspects like companies shall now be able to carry out E-Commerce using Legal Infrastructure for the authentication and origin of electronic communication through digital signatures. However, it is considered the ambiguous law in the area of jurisdiction in the context of the Internet. As sec 1 (2) provides that the act shall extended to the whole of India and save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person. Similarly, sec 75 (2) provides that this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves computer, computer system or computer network located in India. This type of provision appears tobe against the principle of justice. In fact, the term 'cybercrime' at any point even after the amendment by the IT Act Amendment 2008. There is need to push the cyber laws.[9]

1.5 VARIOUS ISSUES UNDER CYBER LAW ENFORCEMENT

Issues related with law

- Territorial jurisdiction is not satisfactory in IT act as jurisdiction has been mentioned in sec 46, 48, 57 and 61 in context of adjudication process and the appellate procedure connected with and again in sec 80 and a part of the police officer power to enter, search a public place for a cybercrime etc. Since the cybercrime are basically computer based crimes and therefore if the mail of someone is hacked in sitting on one place by accused sitting on another Place far in another state, which police station will take the cognizance is difficult to determine because generally investigators avoid accepting complaints on such grounds of jurisdiction.[10]
- Contrary to the real world crimes where tangible evidence in form of weapon of crime, finger prints etc are easy to find and present in court but it is difficult

[9]M.M.Chaturvedi, M.P.Gupta and Jaijit Bhattacharya "Cyber Security Infrastructure in India : A Study" pp.1-15
[10]IDSA Task Report, "India's cyber security challenged" March, 2012

in virtual world to expunge the information from the computer system that what is generally contemplated. This is done with the help of the computer forensics. And the process of preservation of cyber crime evidence lies with the knowledgeable computer forensic expert because any carelessness in the process can lead to diminutive value of the evidence. But it is vital by victim to inform the law enforcement agency as early as possible.

- Experts not only be knowledgeable but also be provided with the technical hardware and software so that they can efficiently fight the cyber crime.
- Law enforcement officers are lack of tools as the old laws are not capable for the crime being committed in the current scenario, new laws hadn't quite caught up to what was happening.
- There is lack of cooperation between the law enforcement agencies and computer professionals.
- The IPC doesn't reveal a term 'cyber crime' at any point even after the IT (amendment) act 2008.
- Lack of security concern in the telecom industry which is integrated into cyberspace, having advert effect of Internet protocol on mobile devices which is considered to be the primary factor for increasing number of attacks.
- Unlike other statutes, policies which are passed by the Indian legislation are not enforceable or binding but merely provide the guidelines for a standard operating procedure. In this regard NCSP doesn't maximize its potential for optimum benefit.

Issues related with the technology

New technology like cloud computing is big concern of cyber threat as for the purpose e-governance and storing data cloud computing is used. The measures taken are not successful to face challenges and risk of cloud computing like:

- Risk of inappropriate access to personal and confidential information.
- Risk of compromise of confidential information and intellectual property
- Appropriate privacy and security measures need to be in place.

Another emerging technology, which is highly in use, is Big Data has critical security and privacy issues. From point of business many works have been carried out focusing on business, application and information processing from Big Data. It's

facing many challenges, such as efficient encrypted and decryption algorithms, encrypted information retrieval, reliability and integrity of Big Data.

1.6FUTURE SCOPE

After going through all these issues and ideology, one can hope that in future some hard and fast laws will be implemented to such crimes so that with the increase in the quantum of punishment, new laws for reference, laws with the specific approach to particular problem, making the individual majority of punishment non bail-able, will help to diminish the rate of cybercrime and the era of technological advancement and digitalization can be free from evil.[11]

With the evolving wave in cybercrime, it is critical to have a cyber law enforcement momentum and cybercrime has the potential to destroy any area of life and it is simple to conduct but very difficult to track. Though India has a highly comprehensive and well-defined legal framework, all of the laws in force in the country were passed long ago, taking into account the particular political, social, economic, and cultural circumstances of the time. Nobody could imagine the Internet at the time. Regardless of our master draftsmen's genius skills, the demands of cyberspace could never be expected. As a result, the Internet's arrival ushered in a slew of delicate legal questions and ills, necessitating the adoption of Cyber rules. Second, even with a liberal analysis, the current legislation should not be viewed in the context of the new cyberspace. The Internet necessitates a legal infrastructure that is compatible with the times. Since current regulations have struggled to provide this legal infrastructure, only the introduction of applicable Cyber laws will provide it. Both of these factors combined to create a favorable environment for India to enforce appropriate cyber laws.

1.7LET'S SUM UP

In this chapter, we have learned the issues with respect to cyber law in India. We have also analysed the legal provisions and how there is lack of enforcement leading to higher number of crime rates. We have also learned about the future scope of the said matter.

[11]David Satola and Henry L.July, "Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework", 'The MW. Mitchell law journal'.

1.8FURTHER READING

- Rohitk Gupta, “An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective”, 2013. [6]Rohit k Gupta, “An Overview of Cyber law vs. Cybercrimes”, 2013.
- PrabhatDalei and TannyaBrahme, “Cyber Crime and Cyber law in India: An Analysis” ‘International journal of humanities and Applied science’ Vol.2 (4), 2014.
- Aashish Kumar Purohit, “Role of Metadata in Cyber Forensic and Status of Indian Cyber Law”, International Journal of computer technology application, vol.2(5) Sep-Oct, 2011.
- M. M. Chaturvedi, M. P. Gupta and Jaijit Bhattacharya “Cyber Security Infrastructure in India : A Study”pp.1-15 [10]IDSA Task Report, “India’s cyber security challenged” March, 2012
- Angshuman Jana and Kunal Kumar Mondal, “A survey of India Cyber Crime and Law and its prevention approach” ‘International journal of Advance Computer Technology’.
- David Satola and Henry L. July, “Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework”, ‘The MW. Mitchell law journal’.

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Mention the risks involved with cloud computing.

Following are the issues related to cloud computing-

- Risk of inappropriate access to personal and confidential information.
- Risk of compromise of confidential information and intellectual property
- Appropriate privacy and security measures need to be in place.

2. Explain cybercrime.

Cybercrime is divided into two categories and defined thus-

(a) Cybercrime in a narrow sense that is computer crime in which any illegal behaviour done by the means of electronic operations that targets the security of computer systems and the data processed.

(b) Cybercrime in a broader sense, which is computer related crime any illegal behavior committed by means of an operating system or network, including such crimes as illegal possession or distributing information by means of a computer system or network.

1.10ACTIVITY

Reflect upon the legal provisions in relation to cyber law in India. (Word count- 2000 to 2500)

Unit 2: EMERGING TRENDS IN CYBER CRIMES IN INDIA: AN OVERVIEW

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Reasons for cybercrimes

2.4 Modes and manners of committing cybercrimes

2.5 Cybercrime and security

2.6 Cyber Warfare

2.7 Let's sum up

2.8 Further reading

2.9 Check your progress: Possible Answers

2.10 Activity

2.1 LEARNING OBJECTIVES

In this chapter we will learn-

- The challenges under cyberspace and various types of cyber crimes
- Various modes and manners to commit cyber crime
- Legal provisions to regulate cybercrime.

2.2INTRODUCTION

Computers and the internet have been an indispensible feature of our lives. Individuals and cultures use them to make life better for themselves. They use them for nearly every part of life, including saving documents, processing data, sending and receiving messages, correspondence, operating computers, typing, editing, painting, and drawing. Cybercrime is described as “unlawful actions in which a computer is used as a weapon, a target, or both”. In the internet, there are several different types of offences. Some aren’t dangerous enough to be classified as a felony, but are just a means of disseminating information. They are merely a display of abilities and are completely harmless. When man created the machine and developed the infrastructure for interacting with machines, he would never have imagined that the virtual space he was building would be filled with cyber-crime. But, by now, nearly everyone has learned of the words digital crime, cyber-crime, ecrime, hi-tech crime, or electronic crime, which refers to any action carried out in cyberspace with a criminal intent.

In basic terms, it is an illegal offense in which a device or network serves as the cause, weapon, goal, or location of the crime. To put it simply, cyber-crime applies to any actions carried out in cyberspace with the intent of committing a crime, as described by the researchers. Unauthorized access, illegal interception by technical means of non-public transmissions of computer data to, from, or inside a computer system, data interference by unauthorized damaging, deletion, deterioration, alteration, or suppression of computer data, and systems interference by interfering with the functioning of a computer are all examples of such crimes involving an information technology infrastructure. In today’s e-Age, “crime” has expanded beyond physical abuse and psychiatric torture to include our online lives. Our lives and surviving in the cyber universe is referred to as E-Life.

Since computers and the internet have become an important part of our personal and professional lives, we are all a part of this cyber universe, whether directly or indirectly. Computers and the Internet, like any other technology, are a blessing to humanity if used correctly and to the benefit of society; otherwise, they are a curse. But, as we all know, everything has advantages and disadvantages, and computers and the internet are no different. If we understand 'Cyber Crime' to be a virus, it is reasonable to conclude that this virus is corrupting man's major creation (computers and the internet), which is responsible for the development of a decent civilization for men. Cybercrime is a global threat that is one of the most difficult and difficult to identify and prosecute. It's worth noting that the official website of the Crime Branch Mumbai's Cyber Crime Investigation Cell notes, "The unseen suspect is more dangerous than the visible criminal."[12]

2.3REASONS FOR CYBER CRIMES

H.L.A. Hart in his work "The Concept of Law" has said 'human beings are vulnerable, so rule of law is required to protect them'.3 Applying this to the cyberspace, we may say that computers are vulnerable, so rule of law is required to protect and safeguard them against cybercrime. Some reasons for the vulnerability of computers are given as under:[13]

1. *Capacity to Store Data in Comparatively Small Space*: The computer has unique characteristic of storing data in a very small space. This makes removing or deriving information either through physical or virtual medium much easier.

2. *Easy Accessibility*: The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers can steal access codes, advanced voice recorders, retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3. *Complexity:* Computers are regulated by operating systems, which are made up of millions of lines of code. The human mind is fallible, and there would almost always

[12] www.newsnish.com/technology/websocial

[13]Nations prepare for cyber war, By David Goldman@ CNN Money Tech, January 7, 2013. http://money.cnn.com/2013/01/07/technology/security/cyber-war/index.html

be a lapse at some stage. Cyber criminals may exploit these flaws to gain access to the computer system.

4*. Negligence:* Negligence is very closely connected with human conduct. It is, therefore, very much probable that while protecting the computer system, there might be any negligence, which, in turn may provide a cyber-criminal an opportunity to gain access and control over the computer system.

5*. Loss of Evidence*: Loss of evidence is a very common & obvious problem as all the data is prone to get destroyed further collection of data outside the territorial extent also paralyses the system of crime investigation.[14]

2.4 MODES AND MANNERS OF COMMITTING CYBER CRIMES

1. Unauthorized Access to Computer Systems: In the broadest context, this kind of crime is referred to as hacking. However, in order to prevent any misunderstanding, the framers of the Information Technology Act of 2000 used this phrase. We wouldn't use the words hacking and unauthorized access interchangeably because the latter has a broader meaning.[15]

2. Theft of Information Contained in Electronic Form: This covers data stored on computer hard drives, portable storage media, and other similar devices. Theft may occur either by physically misappropriating data or by interfering with it through any virtual means.

3. Email Bombing: This kind of activity refers to sending large number of emails to the victim, which may be an individual or a company or even mail servers .This targets at ultimately crashing of the system or the data.

4. Data Diddling: This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is complete. The electricity board faced a similar problem of data diddling while the department was being computerized.

5. *Salami Attacks*: This type of crime is commonly seen in financial institutions and is carried out with the intent of committing financial crimes. A key characteristic of this form of crime is that the change is so minor that it will usually go unnoticed, such as

[14]CYBER WARFARE - Institute for Security Technology Studies. www.ists.dartmouth.edu/docs/cyberwarfare.pdf Similar

[15]http://idsa.in/system/files/book_indiacybersecurity.pdf

in the Ziegler example, where a logic bomb was planted in the bank's system, deducting 10 cents from each account and depositing it in a specific account.

6*. Denial of Service Attack*: In this scenario, the victim's computer is inundated with more requests than it can accommodate, causing it to fail. A distributed denial of service attack is a form of denial of service attack in which the perpetrators are targeted in large numbers and over a large geographic area. Amazon and Yahoo, for example.

7. *Virus Attacks:* Viruses are computer programs that bind themselves to a computer or a file, and spread to other files and devices on a network. They normally have an effect on a computer's data by modifying or removing it. Unlike viruses, worms do not need a host to bind themselves to. They simply make working copies of themselves and replicate the process until they have consumed all of the available memory on a computer, such as the love bug virus, which infected at least 5% of the world's computers. The damages were estimated to be in the amount of $ 10 million. The Internet worm, which was released on the Internet by Robert Morris sometime in 1988 and almost bringing the Internet to a halt, is the world's most popular worm.

8*. Logic Bombs:* There are programs that are triggered by events. This means that these systems are designed to act only when a certain occurrence (referred to as a trigger event) happens. Some viruses are referred to as logic bombs because they are inactive for the majority of the year and only become operational on a certain day (like the Chernobyl virus).

9*. Trojan Attacks:* This phrase comes from the word "Trojan horse." This is a term used in the software industry to describe an illegal program that assumes passive influence of another device by posing as an approved program. The most popular method of Trojan installation is by e-mail; for example, a Trojan was installed in the machine of a female film director in the United States while speaking.

10. Internet Time Thefts: The victim's Internet browsing hours are usually taken up by another user in these types of robberies. This is accomplished by getting access to the login ID and password, for example, in Colonel Bajwa's case, the Internet hours have already been taken up by someone else. This was perhaps one of the first cases of cyber-crime in India to be published. The police, on the other hand, were embarrassed by this case because of their lack of knowledge of the existence of cyber-crime.

2.5CYBER CRIME AND SECURITY

Apart from the dangers of increasing police powers, relying on prosecutors to plan and implement solutions in a highly technical area in which private control is regarded as a substantial advantage may well be ineffective even in satisfying the need for better security. Those who support adoption of a multilateral approach to deal with this quintessentially transnational problem must be encouraged by the fact that states have consistently adopted by the fact that states have consistently adopted multilateral solutions to deal with technologies that affect populations across national boundaries.[16] As technology advances, new technologies with sensational impact that require transnational controls have repeatedly led to multilateral arrangements; agencies have been created to deal with such international areas as air travel, shipping and telecommunication. Transactional needs have demanded transition salutation, which have been satisfied through international agreements on principles, standards, and practices, often developed and proposed by specialized international agencies. States make such arrangements based not upon ideological consideration but on considerations of safety, productivity, and efficient. They have done so, moreover, with no sacrifice of national sovereignty, and almost entirely on the basis of consensus decisions determined by both self -interest and reciprocity.

The information infrastructure faces analogous challenges. Its security and efficiency will be materially increased through international implementation of principles, standards and practices specially designed for this field of activity. The optimum manner of achieving these objectives in this particular field is a multilateral treaty with the necessary commitments to cooperate in investigating and prosecuting an agreed range of conduct, and an international agency with authority to accomplish the legal and technological objectives essential to create a more secure cyber world.

2.6CYBER WARFARE

While there is no universally accepted concept of cyber warfare, it has been observed that states could be attacking other countries' computer systems for

[16]"Statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, FBI on Cyber crime" before the Special Field Hearing, Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Washington, DC

espionage and to destroy their sensitive infrastructure. It mostly applies to politically motivated hacks for sabotage and spying purposes. It is a type of information warfare that is often compared to conventional warfare, though this comparison is debatable in terms of precision and political motive. The assaults on Estonian and Georgian websites in 2007 and 2008 were widely publicized.[17]

While there is no conclusive proof of a state's participation in these attacks, it is generally assumed that non-state actors (such as hackers) were used by state actors. Since these cyberattacks, the topic of cyberwarfare has gained prominence in the international press. The United States has acted quickly to establish a cyber command within the Strategic Forces Command and to update its military doctrine. After ground, air, seas, and space, the US has proclaimed cyberspace to be the fifth dimension of warfare, and has claimed the right to take any action, including nuclear strikes, in response to cyberattacks against it, according to the most recent official military doctrine. Other countries are almost likely to react by following identical military doctrines. The controversy about whether cyber attacks qualify as acts of violence and whether international law on warfare extends to cyber warfare is raging. The question of whether or not there should be codes of conduct for state actors in cyberspace is being debated at the multilateral level.

Since cyberattacks can't be traced back to a single individual, and they affect different computer networks in multiple countries, the problem gets incredibly complicated. The idea of cyber deterrence is still being questioned, but it's unclear if it will work in cyberspace given the ease at which non-state actors can get involved and the lack of attribution. However, there is a continuing controversy between those who think electronic warfare is over-hyped and those who believe the planet is on the verge of a cyber Armageddon.[18]

Both sides have good points, but cyber warfare as a concept has become unavoidable as the number of countries establishing cyber commands continues to rise. These orders have been supplemented by attempts to establish military theories that are applicable. As a result, there is an urgent need to consider electronic warfare rules, whether the rules of armed conflict (LOAC) should be applied to cyber warfare, and how concepts like proportionality and neutrality apply

[17]"Cyber attacks rise from outside and inside corporations", Press Release from Computer Security Institute.
[18]"Ninety percent of survey respondents detect cyber attacks, 273 organization report $265, 589, 940 in financial losses", Press Release from Computer Security Institute, March 22, 2000

in the cyber realm. In the light of cyber warfare, current collective security laws such as Article 41 of the UN Charter and Chapter 7 are considered lacking, especially in terms of the rapidity of cyber-attacks and the excessive time it takes for decision-making and action under these rules.

2.7LET'S SUM UP

In this chapter, we have learned about the types of cybercrimes and various measures to tackle the same. Besides, we also understood the dimension of cyber security in India along with its related relevant provisions.

2.8FURTHER READING

- Noack, David. Computer Viruses Cost $12 Billion in 1999", APB News, Jan. 20, 2000 5. 2. "Love Bug Damage Costs Rise to $6.7 Billion" Press release by Computer Economics, May 9, 2000.
- "Statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, FBI on Cyber crime" before the Special Field Hearing, Senate Committee on Judiciary, Subcommittee on Technology, Terrorism, and Government Information, Washington, DC
- Noack, David. "Businesses Use $12 Billion of Stolen Software" APB News, May 25, 2000, 8. Salkeyer, Alex. "Who Pays When a Business Is Hacked?" Business Week Online: Daily Briefing, May 23, 2000.
- "Cyber attacks rise from outside and inside corporations", Press Release from Computer Security Institute.
- "Ninety percent of survey respondents detect cyber attacks, 273 organization report $265, 589, 940 in financial losses", Press Release from Computer Security Institute, March 22, 2000
- Howe, Carl; McCarthy, John C.; Buss, Tom; and Davis, Ashley. "The Forrester Report: Economics of Security", February, 1998
- Webster's Third New International Dictionary, Merriam-Webster, Inc., Springfield, MA, 1986, page 2442.

2.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is cyber warfare?

While there is no universally accepted concept of cyber warfare, it has been observed that states could be attacking other countries' computer systems for espionage and to destroy their sensitive infrastructure. It mostly applies to politically motivated hacks for sabotage and spying purposes.

2. What is internet theft?

The victim's Internet browsing hours are usually taken up by another user in these types of robberies. This is accomplished by getting access to the login ID and password, for example, in Colonel Bajwa's case, the Internet hours have already been taken up by someone else. This was perhaps one of the first cases of cyber-crime in India to be published. The police, on the other hand, were embarrassed by this case because of their lack of knowledge of the existence of cyber-crime.

2.10ACTIVITY

Reflect upon the types cybercrimes and legal provisions in relation to cyber law in India. (Word count- 2000 to 2500)

Unit 3: STUDY OF LATEST EMERGING TRENDS ON CYBER SECURITY AND ITS CHALLENGES TO SOCIETY

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Latest issue on cyber security

3.4 Recent survey issues on cyber security trends

3.5 Practices and concern by governments for cyber security

3.6 Specific cyber security technologies

3.7 Possible countermeasure techniques

3.8 Key challenges to society

3.9 Let's sum up

3.10 Further reading

3.11 Check your progress: Possible Answers

3.12 Activity

3.1 LEARNING OBJECTIVES

In this chapter we will learn-

- Latest trends on cyber security
- The concerns and measures taken by government.
- Various challenges to the society.

3.2 INTRODUCTION

The Internet is one of the most rapidly developing fields of technical technology. Disruptive innovations such as cloud analytics, social computing, and next-generation mobile computing are radically transforming how businesses use information technology to share information and perform business digitally in today's business world. Since more than 80% of all commercial transactions are now conducted electronically, this area necessitated a high level of protection to ensure transparent and efficient transactions.[19]

Cyber Defense encompasses not just the security of IT applications within the enterprise, but also the wider digital networks on which they depend, such as cyberspace and sensitive infrastructures. In the continuing advancement of information infrastructure and Internet services, cyber security plays a critical role. Enhancing cyber protection and safeguarding sensitive information infrastructures are critical to the security and economic well-being of every nation. Making the Internet better (and protecting Internet users) has been a key component of both new service creation and government policy.A national cyber security and sensitive information infrastructure defense policy would provide measures to deter cybercrime.

As a result, developing and implementing a national policy and plan for cyber defense necessitates a multifaceted approach. Cyber security measures, such as the implementation of technical defense mechanisms or consumer education to discourage them from being victims of cybercrime, can help to reduce cybercrime risk. In the battle against cybercrime, developing and implementing cyber defense solutions is critical.

[19]Anderson, Boehme, Clayton, Moore. (2008). Security Economics and the Internal Market. Available: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

The war against cybercrime necessitates a multifaceted strategy. Given that technological solutions alone cannot deter any crime, law enforcement authorities must be able to successfully detect and prosecute cybercrime.[20]

3.3LATEST ISSUES ON CYBER SECURITY

Privacy and identity theft will remain the most pressing security concerns for businesses. We exist in an environment where all data is stored digitally. Users can connect with friends and relatives in a secure environment on social networking sites. Cybercriminals will continue to hack social media platforms to harvest personal data from home users.[21] There will be new attacks on Android-based smartphones, but they will not be on a large scale. Since tablets and smart phones use the same operating system, they will soon be infected with the same malware as those devices. The number of malware specimens for Macs will continue to rise, but at a much slower rate than for PCs. Windows 8 would enable developers to create apps on almost every Windows-based computer (PCs, laptops, and smart phones), making it easier to create malicious applications similar to those for Android.[22]

Any other day, we hear about cyber-threats such as malware, phishing, and IoT-based attacks. However, enterprises must be mindful that 2020 will bring a whole new level of cybersecurity risks. According to a study by Threat Horizon, organisations will face cyber attacks in the coming years under three main themes –

- Disruption: Relying too much on shaky infrastructure increases the likelihood of planned internet outages that jeopardize business operations. Ransomware can be used by cybercriminals to take control of the Internet of Things.
- Knowledge Distortion: The spread of disinformation by bots and artificial sources would jeopardize interest in the quality of data.
- Deterioration: The capacity of an organization to monitor knowledge would be harmed by rapid developments in smart technology and competing demands raised by changing national security.

Cybercriminals are actively searching for new exploits and devising advanced techniques to defraud and damage institutions and organisations in this era of digital

[20]Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India
[21]Cyber Security Strategy of United Kingdom, 2009
[22]ITU Cyber Security Work Program to Assist Development Countries, 2009

revolution and globalization. In terms of this, companies should be aware of not just the ever-increasing amount of vulnerabilities, but also the looming cybersecurity risks. The details in this post will remind you of the upcoming threats in 2020, allowing you to take preventive steps to mitigate their harm.

3.4RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

The following list was developed from cyber security research and survey

Mobile Devices and Apps

When the number of mobile devices grows, so does the number of security threats. Any new smart phone, tablet, or other electronic computer adds to the number of insecure access points to networks, making them more vulnerable to cyber-attacks. This tragic dynamic is well-known to thieves, who are prepared to strike with highly targeted ransomware and mobile app attacks. Similarly, the issue of lost and stolen computers will grow to cover these modern and outdated technology that historically went unnoticed by cyber security planners.[23]

Social Media Networking

Personal cyber attacks will increase as the use of social media grows. The use of social media for corporations is on the rise, as is the possibility of attack. Organizations should continue to see a rise in the use of social media accounts as a platform for social engineering strategies in 2012. Companies would need to look beyond simple protocol and practice implementation to more sophisticated capabilities including data leakage protection, improved network management, and log file review to combat the threats.

Cloud Computing

Cloud computing is a new technology that brings different types of services under one roof. Cloud computing provides services over the internet and the client pay according to their usage. Suppose you want to travel from New York to London you do not need to own or purchase a plane. Instead of this you book a ticket and pay for the airline, according to your destination. The rest of the things will be managed by the airline staff. The same working model is adopted by cloud computing. In cloud computing you pay for what you use the rest of the things will managed and

[23]Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005

maintained by cloud providers. In cloud computing concept different entities play the different role according to its need. These entities system can be multi layer to basic three layer model.

In basic three layer model of cloud computing Consist: Client, Cloud Service Provider and Cloud Host Company.

i. ***Client:*** A Client is an entity that uses the service from the provider to solve their business computing problems. It can be considered as an end user. The Consumer access the provider's service, either through the API or Internet Connection. A cloud consumer is charged on the basis of usage according to Pay-per-use Model.

ii. ***Cloud Service Provider***: A Provider is usually a third party that makes services available for a customer. A cloud service provider working as a bridge between the end user and the cloud Host company. It maintains the required infrastructure and capabilities to deliver service to the customer. The capabilities vary based on the type of cloud service the provider delivers.

iii. ***Cloud Host Company***: An intermediary works on the behalf of Cloud consumers to deal with the provider. It helps the consumer to architect the right system on a cloud provider, and assists in all activities of a provider and consumer.

Cloud storage can be used for more businesses. Cloud computing's huge cost savings and efficiencies are convincing businesses to move to the cloud. Organizations would be able to better handle the challenges of cloud computing if they have a well-designed infrastructure and internal security preparation. Unfortunately, recent polls and studies show that businesses underestimate the value of protection due diligence while vetting these vendors. If the number of people using the cloud grows in 2012,[24] new breach cases will demonstrate the difficulties that these services face for forensic investigation and incident management, and cloud protection will hopefully get the recognition it deserves.

Protect systems rather Information

The emphasis will be on information security rather than machine security. As customers and companies increasingly store important information electronically,

[24]ArunPrabhudesai, "Cyber Attacks In India", 2011

protection considerations can expand from merely handling systems to securing the data these systems contain. Rather than concentrating on designing processes to secure the databases that store information, consumers and businesses would require more granular control of the data stored there.

New Platforms and Devices

Cybercriminals would have additional openings as a result of new platforms and computers. Personal computers running Windows have long been concerned with security risks. However, the introduction of emerging platforms and smart phones - such as the iPhone, iPad, and Android - would almost certainly result in new challenges. This summer, the first Android phone was infected with a Trojan, and rumors of malware software and spyware continue to surface, not just on Android.[25]

Everything Physical can be Digital

Printed notes on a sheet of paper, journal binders, and even pictures on the wall can be copied in digital format and gleaned for the tools to enable an activist-style security breach, and this will become increasingly a challenge.

3.5PRACTICES AND CONCERN BY GOVERNMENTS FOR CYBER SECURITY

Ensure the national cyber security strategies take into account the interests of all people, not just those of central government. Encourage adoption and implementation of the Cybercrime Convention and other proposed international treaties. Support end-user education because it not only supports the actual user and scheme, but it also decreases the amount of vulnerable machines that can be hijacked by hackers and used to launch assaults. Influence computer industry vendors to supply professionally validated hardware and applications by using procurement control, standard-setting, and licensing. Increase the number of specialized police and forensic computing services available. As the most likely way of averting or mitigating a large-scale Internet crisis, support the international Computer Emergency Response Team (CERT) group, even by funding. Strengthened Internet protocols, Risk Analysis, Contingency Planning, and Disaster Propagation Analysis, Human Factors in the Use of Computer Technology, and Security Economics are all fields where research is required.

[25]GAO (2010), Cyberspace, United States faces Challenges in Addressing Global Cybersecurity and Governance, GAO-10-606 http://www.gao.gov/products/GAO-10-606

3.6SPECIFIC CYBER SECURITY TECHNOLOGIES

Access Control and Identity Management - The username/password combination has been a fundamental of computer access control since the early 1960s.[26]

Authentication- Documents need to be authenticated as having originated from a trusted source and that they have not been subsequently altered.

Malware scanners-Software that is regularly scans files and messages for malicious code.

Firewalls- A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorized usage.

Cryptography-It is used in information management in two ways. The more well-known method is to provide secrecy by encrypting all saved and transmitted data.

3.7POSSIBLE COUNTERMEASURE TECHNIQUES

Users and organisations will improve their preparation and response to better protect against a variety of threats and mitigate the possible impacts of attacks by following good cyber protection practices:[27] Make sure your smart phones and other electronic devices have encryption and password features available. Configure and patch operating systems, browsers, and other device applications correctly. Firewalls, anti-virus, and anti-spyware applications can all be included and modified on a daily basis. Always be careful when communicating with others; deliberate before you press. On social media platforms, don't share too much personal knowledge about yourself. You may become a victim of identity theft or property theft depending on the details you share. When unauthorized contact or actions are discovered, report them to Internet service providers and local law enforcement.

3.8KEY CHALLENGES TO SOCIETY

Public and private agencies in the fields of public health, emergency care, administration, defense industrial base,[28] information and telecommunications, electricity, transportation, banking and finance make up our nation's vital infrastructures. India's dependence on technology is also reflected in the fact that the

[26]Information Warfare Monitor (2010), Shadows in the Cloud, www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2- 0

[27]Mukhopadhyaya, K and Sinha, B P. (1992). Reliability analysis of networks using stochastic model . Information Sciences . Volume 65, Issue 3, 225-237 .

[28]OECD (Organisation for Economic Cooperation and Development) (2002), OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Recommendation of the Council adopted 25 July 2002, OECD, Paris.

country is changing gears by dabbling in e-government. India has now embraced e-government in areas such as income tax and passports and visas. Sectors such as law enforcement and the courts will be followed. This is indeed a big deal in the tourism industry. The majority of Indian banks have completed full computerization. E-commerce and e-banking have since been introduced as a result of this. The financial markets haven't been spared yet.

Cybercrime has evolved into an extreme, pervasive, violent, rising, and increasingly advanced threat to national and economic security. Many businesses, institutions, public and private-sector entities (especially those involved in essential infrastructure) are in grave danger. Having the Cyber Security stance correct around the board would be critical for future growth, creativity, and competitive advantage for both companies and governments. Businesses will be able to work for a potential world that is both transparent and stable and prosperous by collaborating through public and private sector alliances and advancing security policies, especially with regard to mission-critical networks, procedures, and technologies that are linked into cyberspace.

3.9LET'S SUM UP

In this chapter, we have learned various terminologies including cloud computing, data protection, social media networking etc. Additionally, we have analysed latest trend on cyber security and its interface with possible countermeasure techniques.

3.10FURTHER READING

- Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India
- Yang, Miao, "ACM International Conference Proceeding Series", vol. 113
- Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011
- Cyber Security Strategy of United Kingdom, 2009
- ITU Cyber Security Work Program to Assist Development Countries, 2009, Rev. Jonames Burg, TTU WTSA Resolution 50, 2008
- ITU Cyber Security Work Program to Assist Development Countries, 2008
- Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2

- Schjolberg / Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, 2005
- The most Important Instruments in fight against Cybercrime, Ch. 6.2
- Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012
- ArunPrabhudesai, “Cyber Attacks In India”, 2011
- Audry Watters, Read Write Cloud, RWW Solution Series, 2010

3.11CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Explain the scope of Cyber security.

Cyber Defense encompasses not just the security of IT applications within the enterprise, but also the wider digital networks on which they depend, such as cyberspace and sensitive infrastructures. In the continuing advancement of information infrastructure and Internet services, cyber security plays a critical role. Enhancing cyber protection and safeguarding sensitive information infrastructures are critical to the security and economic well-being of every nation.

2. Highlight latest cyber security issue.

There will be new attacks on Android-based smart phones, but they will not be on a large scale. Since tablets and smart phones use the same operating system, they will soon be infected with the same malware as those devices. The number of malware specimens for Macs will continue to rise, but at a much slower rate than for PCs. Windows 8 would enable developers to create apps on almost every Windows-based computer (PCs, laptops, and smart phones), making it easier to create malicious applications similar to those for Android.

3.12ACTIVITY

Elaborate specific cyber security technology along with its interface with latest trends. (Word count- 2000 to 2500 words)

Unit 4: CHALLENGES TO ENFORCEMENT OF CYBER-CRIMES LAWS AND POLICY

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Motivation for cybercrime

4.4 Cybercrime statutes

4.5 Challenges to enforcement of cybercrime.

4.6 Dearth of experts in prosecution of cybercrimes

4.7 Let's sum up

4.8 Further reading

4.9 Check your progress: Possible Answers

4.10 Activity

4.1 LEARNING OBJECTIVES

In this chapter we will learn-

- Reasons for committing cybercrimes.
- Various challenges in enforcement of cybercrime.
- Legal provisions/statutes with respect to the regulation of cyber crime.

4.2 INTRODUCTION

Cyber-crimes are a relatively new phenomenon, but they have become the focus of global attention simply because all citizens of the world, whether private or public, are vulnerable to them. This vulnerability is almost unavoidable because the world is in an information age (Encyclopaedia of Library and Information Science, 1977), and cyber-crimes emerged with the advent of the internet. To begin, it is important to make a brief distinction between a computer crime and a cyber-crime, the reason being that the two terms are often confused as one and the same, when in reality they are just identical but distinct.[29]

Computer crimes are crimes committed using a device; in other words, computer crimes include crimes committed against the computer hardware, the materials contained or connected with the computer, such as software and data; common examples of computer crimes include embezzlement, theft, financial manipulation, and hacking, among others. Cyber-crime is a catch-all word for two types of crimes: cyber-dependent and cyber-enabled (McGuire and Dowling, 2013). Cyber-dependent crimes are those that can only be committed through the use of a data, computer networks, or some means of ICT.[30]

The definitional problem of cybercrime persists, yet one thing is certain: most definitions of cybercrime make reference to the Internet; for the sake of overcoming the dichotomies in jurisdictions and still addressing the same concept in legal literature, cybercrime has no globally accepted definition that might possibly encapsulate all the facets of this novel brand of crime.Cybercrime, according to the

[29]Ahamad M, Amster D, Barrett M, Cross T, Heron G, Jackson D, King J, Lee W, Naraine R, Ollmann G, Ramsey J, Schmidt HA, Traynor P (2008). Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Centre. Georgia Inst. Technol. 9p.

[30]Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2810782 or http://dx.doi.org/10.2139/ssrn.2810782

Oxford Dictionary of Law (2002), is any criminal or other offence that is encouraged by or involving the use of electronic media or computer networks, such as any computer or the Internet, or any one or both of them.

4.3MOTIVATIONS FOR CYBERCRIME

Such cybercrime consequences include but are not limited to loss of intellectual property and sensitive data, cost of opportunity including service and employment disorder, brand image and company reputation, penalties and compensatory payments to clients, in addition to the global financial losses outlined in the paragraphs above (Paganini, 2013).After highlighting the impact of cybercrime in terms of financial and economic impacts,[31] as well as other repercussions, the appropriate concern that will inevitably agitate the mind of a thoughtful individual is: what are cybercriminals' motivations?

The following is a brief response to this important issue: The profit motive seems to be the first and most important motivation for cybercriminals to continue their nefarious activities of infiltration or unauthorized interference with computers and network systems; the profits accruing to cybercriminals are enormous; as previously said, the financial losses at the global level are profits to cybercriminals.[32] The difficulty of detecting cybercriminals is closely related to the profit motive; the Internet provides a broad range of freedom for all citizens of the world, and the lack of a requirement of identification as to who is doing what, through the use of telecommunications through cyberspace, continues to thwart global efforts aimed at tracking criminals and bringing them to justice.

Competitors bolster cybercriminal activity by sponsoring attacks on one another, whether by hacking to steal sensitive knowledge about trading secrets or distributed denial of service attacks to cripple a competitor's service (DDoS). It should be noted that certain cybercriminals are motivated solely by the satisfaction or pleasure they derive from gaining unauthorized access to computers and computer networks; the very fact that cybercriminals are able to gain access to computer systems that the owners and operators believe to be safe and secure, thus revealing vulnerability,

[31]Centre for Strategic and International Studies (CSIS) (2014). Net Losses - Estimating the global cost of cybercrime. Economic impact of cybercrime II. June 2014. pp. 1-24. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf

[32]Chang W, Chung W, Chen H, Chou S (2003). An International Perspective on Fighting Cybercrime, ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics. pp. 379- 384.

gives the cybercriminal a competitive advantage. Finally, a threat or protest against computer networks, which is an external expression of registering disagreement or criticism against owners or administrators, is another type of incentive for cybercriminals. This type of motivation is more often than not directed at profiting from cybercriminal activities.

4.4CYBERCRIME STATUTES

Cybercrime seems to be well known to the ordinary Internet savvy citizen anywhere he is located on the globe; nevertheless, the idea of cybercrime has no universally recognized meaning. Cybercrime, on the other hand, is described as the use of a device with an Internet connection to commit online crimes.[33] In light of the above, this paper defines cybercrime as illicit internet-mediated practices that often occur in global electronic networks (Chang et al., 2003). There are many forms of cybercrimes and for ease of reference, it includes but not limited to 419 emails and letters, advance fee fraud, online auction fraud, online betting fraud, botnet-related fraud, child pornography and related offences, computer hacking, computer related forgery, computer related fraud, cracking, credit card fraud, cyber-laundering, cyber-smearing, cyber piracy, cybersquatti, Trojan horse, spyware, system interference and vishingare only a few examples of cybercrime.[34] Many sovereign countries around the world have policies in place to deter, regulate, criminalize, investigate, and prosecute cybercrime, and those who do not are working to pass regulations to address the threat faced by cybercrime. Hereunder is a summary of measures embarked upon at international and regional levels to address cybercrimes:

In 1997, the G8 released a Ministers' Communiqué outlining an action plan and principles to fight cybercrime and secure data and networks from unauthorized access. It also stated that all law enforcement officers must be prepared and ready to deal with cybercrime, and that all member countries must have a point of touch available 24 hours a day, seven days a week (Chang, 2003). In 1990, the United Nations (UN) General Assembly passed a resolution on electronic crime law. It also passed a resolution in 2000 to curb criminal misuse of information technology, and a

[33]Convention on Cybercrime (2001). Summary of the treaty, European Convention on cybercrime. Available at: ftp://ftp.freenet.at/privacy/gesetze/europarat-cybercrime-summary.pdf

[34]Ernst, Young (2003). Fraud: Unmanaged risk. 8th global survey. Global investigations dispute advisory services, South Africa. Available at: https://www.whistleblowing.com.au/information/documents/EY8thGlobalSurvey2003.pdf

second resolution in 2002 to tackle criminal misuse of information technology (Nicholas, 2008).

The International Telecommunication Union (ITU), which is responsible for tele-communications and cyber security matters at the United Nations, issued the Geneva Declaration of Principles and Plan of Action in 2003, stressing the relevance of interventions in the battle against cybercrime, and in 2005,[35] the Tunis Commitment and Tunis Agenda for the Information Society. In 2001, the Council of Europe (CoE), which comprises 47 European member states, took the lead by establishing the first international Convention on Cybercrime, which was drafted in collaboration with the United States, Canada, and Japan and signed by 46 member states but only ratified by 25. (Ahamad et al., 2008).[36] The Convention, also known as the Budapest Convention, is the first transnational settlement on crimes committed through the Internet and other electronic networks, focusing on copyright infringements, computer-related piracy, child pornography, and network security breaches which also include a number of forces and processes, such as computer network search and interception.

4.5CHALLENGES TO ENFORCEMENT OF CYBERCRIMES

The efforts made by the instrumentality of legislations at national, international, and regional levels were discussed previously; without prejudice to the effectiveness of the existing laws in place to combat cybercrime, the scourge persists, nay, rather than the laws to curb, or better still, minimize cybercrime, there is a rise in the frequency and sophistication of cybercrime, and the reason for this is that cybercrime is becoming more sophisticated. Here, the challenges faced by mankind which makes cybercrimes intractable are discussed as follows:

Identity of cybercriminals

There is no simple way of determining who is doing what and where an Internet user is located at any given time; the global information system is open, and there are no prerequisites that must be met before a user can communicate with others, anywhere on the planet. As a result of the unrestricted freedom of information and

[35]International Telecommunication Union (2009). Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Sector. https://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[36]McGuire M, Dowling S (2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom, October. 30p.

correspondence, cybercriminals may conceal their identities using various telecommunications devices, making it difficult to track a user's online Internet Protocol (IP) address. Furthermore, even if a cybercriminal's IP address can be traced to a specific location, the next barrier cannot be overcome because a cybercriminal's identity is unknown to the owner or user of the Internet service provider.

Jurisdictional challenges

Aside from the important problem of privacy previously mentioned, another formidable obstacle to the prosecution of cybercrime legislation is authority. Taking into account the time-tested values of state freedom, autonomy, and territorial integrity, each nation-state in the world has the authority to enact laws that apply to all objects and people within its geographical entity, referred to as a territory. Conflict of laws is inevitable due to the above cause of nation-states passing laws on the same subject from separate jurisdictions. The power of a court or judge to entertain an action, appeal, or proceeding is known as jurisdiction. The question of jurisdiction is so fundamental that it serves as the foundation for every decision, or, to put it another way, it goes to the heart of every case before the courts. A court that lacks authority therefore lacks the requisite competence to hear the appeal. A lack of integrity renders the litigation null and void from the start, regardless of how well-run and settled the case might be.[37]

Extradition processes challenge

The term extradition is made up of two French words: ex, which means "out," and custom, which means "deliverance." That is the method of a new judicial jurisdiction recalling someone convicted of a crime for conviction or punishment. Extradition is often known as the surrender of a person convicted of committing an offense in one state to another (Oxford Dictionary of Law, 2002).A cursory glance at the above definition of extradition might lead one to believe that if a person is accused of committing a cybercrime in one jurisdiction and flees to another, all that is required of the country where the cybercriminal is domiciled is to quickly return the said criminal to the requesting country to face trial; however, in practice, this is not the case.

[37]Nicholas CAMQC (2008). Emerging Trends in Cyber Crime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities, International Association of Prosecutors, Singapore. Available at: http://www.odpp.nsw.gov.au/docs/default-source/speeches-bynicholas-cowdery/emerging-trends-in-cyber-crime.pdf?sfvrsn=2

There is no instrument of international law that requires sovereign states to automatically return cybercriminals for prosecution. In effect, countries where cybercriminals are located often fail to extradite cybercriminals for various reasons, and this trend poses an insurmountable obstacle to the global implementation of cybercrime laws.

4.6DEARTH OF EXPERTS IN PROSECUTION OF CYBERCRIMES

The lack of expertise in the investigation of cybercrimes is linked to the above causes of insufficient experience, remuneration, and inadequate security and safety on the dangerous job for law enforcement agency officers. It is a well-known fact that, even though law enforcement agencies did a good job investigating cybercrime,[38] at the litigation stage, the expertise of prosecution attorneys is also critical in securing the conviction of a cybercriminal and it is incumbent on prosecution to prove his case beyond a reasonable doubt; unfortunately, this is not the case because there is a scarcity of savvy prosecutors in the country.

Cybercriminals, on the other hand, have unrestricted access to renowned private prosecutors that demand exorbitant defense rates, which is not a challenge for them since they can easily afford to pay large professional fees to the finest cybercrime lawyers. Furthermore, the anonymity issue of cybercriminals, as well as the nature of evidence, which is often shaky due to the fact that investigators can only rely on traces and tracks left on computers and the Internet, all add to the case of prosecutors who are not as well-versed in handling cybercrime litigation as their private practice counterparts; these identified gaps are unfortunate.

4.7LET'S SUM UP

In this chapter, we have learned various challenges to enforcement of cybercrime. We have also worked on multiple concepts surrounding cybercrime. Besides, we analysed the position in USA and its similarity with Indian context.

[38]Paganini P (2013). InfoSec Institute 2013 Cost of cybercrimes http://resources.infosecinstitute.com/cybercrime-and-theunderground-market/

4.8FURTHER READING

- Ahamad M, Amster D, Barrett M, Cross T, Heron G, Jackson D, King J, Lee W, Naraine R, Ollmann G, Ramsey J, Schmidt HA, Traynor P (2008). Emerging Cyber Threats Report for 2009, Georgia Tech Information Security Centre. Georgia Inst. Technol. 9p.
- Ajayi EFG (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. International Journal of Information Security and Cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015- issue-2-article-4/ Ajayi EFG (2016). The Impact of Cybercrimes on Global Trade and Commerce.
- Bassiouni MC (1999). The Sources and Content of International Criminal Law: A Theoretical Framework, 1 International Criminal Law 3-126. 2:353-356
- Centre for Strategic and International Studies (CSIS) (2014). Net Losses - Estimating the global cost of cybercrime. Economic impact of cybercrime II. June 2014. pp. 1-24. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impactcybercrime2.pdf Chang W, Chung W, Chen H, Chou S (2003).
- An International Perspective on Fighting Cybercrime, ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics. pp. 379-384.
- Commonwealth, Litigation Practice (1962). Macfoy versus United Africa Company Limited (West Africa). PC 27 NOV 1961.

4.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is Extradition?

The term extradition is made up of two French words: ex, which means "out," and custom, which means "deliverance." That is the method of a new judicial jurisdiction recalling someone convicted of a crime for conviction or punishment. Extradition is often known as the transfer of an individual convicted of committing an offense in one country to another.

2. Define Cybercrime

Every criminal or other offence facilitated or involving the use of electronic messages or computer systems, including any software or the Internet, or any more or more of them, is referred to as cybercrime.

4.10 ACTIVITY

Elaborate specific reasons for challenges in enforcement of cybercrime. (Word count- 2000 to 2500 words)

Block-2

ARTIFICIAL INTELLIGENCE AND CYBER LAW

Unit 1: THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Historical Attempts

1.4 Knowledge or Rule-Based Approach

1.5 Pattern Recognition Approach

1.6 Machine learning

1.7 Supervised Machine Learning

1.8 Unsupervised Learning

1.9 Cyber security

1.10 Role of Cyber security

1.11 Principles of Cyber Security (Principles Forming the Base for Cyber security)

1.12 Let's sum up

1.13 Further reading

1.14 Check your progress: Possible Answers

1.15 Activity

1.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- The relationship between Artificial intelligence and Cyber security
- Concept of machine learning.
- Detailed analysis of cyber security.

1.2 INTRODUCTION

In the modern age, cyber defense has become a big concern. Data hacks, identity fraud, captcha breaking, and other such reports abound, involving millions of people as well as businesses. The challenges have always been endless in terms of devising appropriate controls and protocols and putting them in place with pinpoint accuracy in order to combat cyber threats and crimes. With recent advances in artificial intelligence, the possibility of cyber threats and crimes has increased exponentially. It has been used in almost every scientific and engineering area. AI has revolutionized everything from hospitals to robots. Since cyber criminals couldn't keep this ball of fire from them, "normal" cyber attacks have evolved into "intelligent" cyber attacks.[39]

"Intelligence" is only one of the characteristics that separates humans from all creatures on the globe. While machines cannot have that inherited intellect, the thought of getting that intelligence in man-made machines is intriguing. Instead of normal human intellect, scientists, philosophers, and those working to explain the human mind began to wonder, "Why can't robots think?" The concept of developing "Artificial Intelligence" started to draw the interest of scholars all over the world as a result of multidisciplinary activities in brain science, neuroscience, and computer science.

Researchers began to have high hopes for AI science in the 1960s and 1970s, but they were mostly disappointed because no breakthroughs were made. Artificial intelligence can be described as a scientific area that attempts to understand and model human intelligence. Many researchers have their own interpretations of AI, citing Artificial Intelligence: A Modern Perspective by Peter Norvig and Stuart Russell

[39]Bhatele, Kirti Raj &Shrivastava, Harsh. (2019). The Role of Artificial Intelligence in Cyber Security. 10.4018/978-1-5225-8241-0.ch009.

as an example.[40] “The analysis of agents that live in the world and understand and behave is known as Artificial Intelligence.” For decades, there has been a push to develop technologies that can perceive, think, read, and act like humans.

1.3HISTORICAL ATTEMPTS

For the first time in 1943, Warren McCulloch and Walter Pitts tried to construct an intelligent device. They suggested a model of an artificial networked neural system, claiming that if properly defined, it might learn in the same way as the human brain. Alan Turing wrote “Computer Machinery and Intelligence” a year ago, in which he discussed the concept of “Artificial Intelligence.”[41] He also suggested the “Turing test” as a way to calculate a machine’s ability to exhibit intellect in his work. The examination involves a computer that generates natural language, an evaluator (who is human), and a human. The evaluator can converse (interact) with both the computer and the person in order to classify the machine. Both the computer and the human will attempt to convince the evaluator that they are conversing with another human. If the evaluator is unable to differentiate between computer and human conversation, the machine would be deemed intelligent.

In 1956, John McCarthy invented the word “Artificial Intelligence.” He developed LISP, a high-level AI programming language for use in AI applications, two years later. We’ll go over one of the most commonly used AI approaches in the next section, and then we’ll go over the latest and strongest AI approach (Pattern Recognition).

Artificial Intelligence has the potential to provide large incremental value to a wide range of sectors globally, and is expected to be the key source of competitive advantage for firms.

a) Healthcare: Application of AI in healthcare can help address issues of high barriers to access to healthcare facilities, particularly in rural areas that suffer from poor connectivity and limited supply of healthcare professionals. This can be achieved through implementation of use cases such as AI driven

[40]Bai, J., Wu, Y., Wang, G., Yang, S. X., &Qiu, W. (2006). A very distinctive intrusion detection model based on multilayer self-organizing maps and principal part analysis. In Advances in Neural Networks. Springer.

[41]Chatzigiannakis, V., Androulidakis, G., &Maglaris, B. (2004). A Distributed Intrusion Detection Prototype Using Security Agents. In Proceedings of Workshop of the HP Open View University Association. University of Evry.

diagnostics, personalised treatment, early identification of potential pandemics, and imaging diagnostics, among others.

b) Agriculture: AI holds the promise of driving a food revolution and meeting the increased demand for food (global need to produce 50% more food and cater to an additional 2 billion people by 2050 as compared to today). It also has the potential to address challenges such as inadequate demand prediction, lack of assured irrigation, and overuse / misuse of pesticides and fertilisers. Some use cases include improvement in crop yield through real time advisory, advanced detection of pest attacks, and prediction of crop prices to inform sowing practices.

c) Smart Mobility, including Transports and Logistics: Potential use cases in this domain include autonomous fleets for ride sharing, semi-autonomous features such as driver assist, and predictive engine monitoring and maintenance. Other areas that AI can impact include autonomous trucking and delivery, and improved traffic management.

d) Retail: The retail sector has been one of the early adopters of AI solutions, with applications such as improving user experience by providing personalised suggestions, preference-based browsing and image-based product search. Other use cases include customer demand anticipation, improved inventory management, and efficient delivery management.

e) Manufacturing: Manufacturing industry is expected to be one of the biggest beneficiaries of AI based solutions, thus enabling 'Factory of the Future' through flexible and adaptable technical systems to automate processes and machinery to respond to unfamiliar or unexpected situations by making smart decisions. Impact areas include engineering (AI for R&D efforts), supply chain management (demand forecasting), production (AI can achieve cost reduction and increase efficiency), maintenance (predictive maintenance and increased asset utilisation), quality assurance (e.g. vision systems with machine learning algorithms to identify defects and deviations in product features), and in-plant logistics and warehousing.

f) Energy: Potential use cases in the energy sector include energy system modelling and forecasting to decrease unpredictability and increase efficiency in power balancing and usage. In renewable energy systems, AI can enable

storage of energy through intelligent grids enabled by smart meters, and also improve the reliability and affordability of photovoltaic energy. Similar to the manufacturing sector, AI may also be deployed for predictive maintenance of grid infrastructure.

g) Smart Cities: Integration of AI in newly developed smart cities and infrastructure could also help meet the demands of a rapidly urbanising population and providing them with enhanced quality of life. Potential use cases include traffic control to reduce congestion and enhanced security through improved crowd management.

h) Education and Skilling: AI can potentially solve for quality and access issues observed in the Indian education sector. Potential use cases include augmenting and enhancing the learning experience through personalised learning, automating and expediting administrative tasks, and predicting the need for student intervention to reduce dropouts or recommend vocational training.[42]

1.4KNOWLEDGE OR RULE-BASED APPROACH

We aim to embed the expertise of human experts for decision-making in Knowledge-based AI systems. The aim is to give the machine the information it needs to perform a mission, such as medical diagnosis, as well as the guidelines it needs to infer ideas from that knowledge and make a decision.[43] All of the decisions made by the KBAI algorithm would be influenced solely by the knowledge base provided by a human expert in the field. As a result, KBAI systems are often referred to as Expert Systems. As a result, the KBAI system's general architecture consists of a Knowledgebase and an Inference Engine. For inference from the knowledge base, most inference engines use IF-ElSE laws. MYCIN was the first knowledge-based method. It was created for the purpose of medical diagnosis. The fundamental idea behind information-based structures was to specifically interpret knowledge using IF-ElSE laws (Russell, S., J., &Norvig, P., 2000). The role of designing an AI system

[42]http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf
[43]Bostrom, N. (2015), TED Talk on Artificial Intelligence. Retrieved from https:// en.tiny.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_ smarter_than_we_are

revolves around the representation of information. The rule-based information representation was heavily used in IBM Watson's production.[44]

1.5PATTERN RECOGNITION

Another path to Artificial Intelligence is pattern analysis. In contrast to the rule-driven approach, it is based on results. It tries to derive information from the results. To discover patterns from the data, we just need data and a machine learning algorithm (section 2). These patterns can be used to derive the system's decisions in an uncertain world. The following is a modern example of pattern identification (according to Bishop): The field of pattern recognition is concerned with the automated detection of regularities in data using computer algorithms, as well as the use of these regularities to perform activities such as data classification. The best approach to Artificial Intelligence has been pattern detection. When it comes to pattern recognition, machine learning is the most effective method. We'll go into it in detail in the next segment (Russell, S., J., &Norvig, P., 2000).

1.6MACHINE LEARNING

The last innovation that mankind will ever need is machine intelligence (Bostrom, N., 2015) Arthur Samuel invented the term "machine learning" in 1959. "Machine learning is the area of research that enables the robot to learn without being directly programmed," he says. This concisely expresses the central concept. Unlike previous methods that attempted to specify a large number of laws in order to gain information from data, machine learning creates systems that learn certain rules from the data themselves. This method is more akin to normal learning.[45]

A child, for example, learns to recognize an apple after being given several examples of apples. Similarly, we provide a large amount of data to the computer, and the machine develops an understanding for the data on its own. "A computer program is said to benefit from experience E with respect to any class of tasks T and output measure P if its performance at tasks in T, as measured by P, increases with experience E," according to Tom Mitchell. The Machine learning algorithm refers to

[44]Iftikhar, B., &Alghamdi, A. S. (2009). Application of artificial neural network within the detection of dos attacks. Proceedings of the ordinal international conference on Security of knowledge and networks, 229–234.
[45]Kivimaa, J., Ojamaa, A., &Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. Proceedings of Military communications conference, MILCOM 2008.

the algorithms that enable machines to learn. In general, there are two types of machine learning algorithms: supervised learning and unsupervised learning (Russell, S., J., &Norvig, P., 2000). Other types of machine learning include reinforcement learning and others.

1.7SUPERVISED MACHINE

Educating yourself the data is named in supervised learning. Let's assume we want the machine to be able to tell the difference between photographs of cats and other images. We'll write a program that takes an image as input and determines whether or not it's a cat (i.e. 1 for cat and 0 for non-cat). We must first train the computer in order to complete this mission. This means that for a huge number of photographs, we'll first show the computer that this is a cat image, this is a noncat image, and so on.[46] Then we'll assess how well it does on pictures it has never seen before. If the performance falls short of our expectations, we will retrain it with more details. The data used for preparation is referred to as the "training package," while the data used to assess the learned structure or "Model" is referred to as the "testing set." The term "Sample" refers to data examples of photographs. In the supervised learning setup, each sample has a matching true mark. The topic we discussed is referred to as "Classification," because there are only two classes: cat and non-cat.

It's called "Binary Classification" where there are just two classes, and "Multi-class classification problem" when there are more than two classes. In contrast to the classification issue, we want our regression method to forecast "continuous values." Predicting house prices in a neighborhood, for example. What information do we need to gather in this scenario? We'll try to gather information on the factors that influence house prices, such as house size, number of rooms, and so on. In machine learning language, the parameters are referred to as "Features." We'll also include real sample prices in the training set, but not in the evaluation set (obviously, this is the data we use to test our system). Another example of regression is forecasting stock exchange values. Another classification example may be used to determine

[46]Jonze, S. (2017). 28 Best Quotes About Artificial Intelligence. Retrieved from https:// www.forbes.com/sites/bernardmarr/2017/07/25/28-best-quotes-about-artificialintelligence

whether or not an individual has cancer.[47] You came up with the concept (Russell, S., J., &Norvig, P., 2000).

1.8UNSUPERVISED LEARNING

We don't have the sample's true mark or meaning in unsupervised learning. The information is not classified. The unsupervised learning algorithm's goal is to discover structure in the input data. Its aim is to uncover secret trends in data. It attempts to organize the data into distinct categories based on their characteristics (Russell, S., J., &Norvig, P., 2000). Clustering is the term for this mission. Let's take a look at how this is beneficial. A publishing house wishes to increase its revenues. It has a vast array of information on its consumers' purchasing habits. The company feeds the data into a "Cluster" learning algorithm, which produces 5 consumer segments, and the company discovers that the first segment enjoys romantic genre books, the second enjoys x genre books, and so on. With this knowledge, the organization will tailor its offering to specific business segments. Clustering methods have been used in astronomy, computer science, and other fields.

1.9CYBER SECURITY

Consider a package, for example (Artificial Intelligence, Machine Learning, Block Chain, Deep Learning, Big Data Analysis, Data Science, Internet of Things etc.). This collection includes some of today's most exciting and talked-about developments. In this period of rapidly growing Internet growth and intense workloads in the fields mentioned above, cyber-security has become a major concern.

The word "cyber" refers to "computer culture, information media, or/and virtual reality." This makes it clear that we're about machine, network, and information security. To clarify, cyber security refers to the different measures/techniques used to secure integrated networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage).Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes

[47]Kivimaa, J., Ojamaa, A., &Tyugu, E. (2009). Graded Security accomplished System. In Lecture Notes in engineering (Vol. 5508, pp. 279–286). Springer.

components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure. This architecture resembles a multilayer security scheme that is distributed across the system and involves different system components, and it is one of the most effective defensive mechanisms possible.[48]

1.10ROLE OF CYBERSECURITY

Thanks to the evolving existence of cyber-risks, the general public is becoming more vulnerable to cyber-attacks. Pathways are built by malicious and aggressive practices that grant predators (hackers and crackers) unwanted access to computer systems or networks. Cyber attacks are the term for these types of operations. To create these paths, predators focus on the system's or network's glitches and flaws. Ransomware, malware, worms, Trojans, spyware/adware, attack vectors, social engineering, Man in the Middle (MITM), and other cyber threats abound (Panimalar, A., Giri, P.U. & Khan, S., 2018).[49]Everyone has important assets and sensitive data under their control, and when an individual gains access to those assets and data, they may do significant harm. In the case of cyberspace, these unauthorized accesses may be the product of one or more cyber attacks. Here's where cybersecurity falls through. It ensures your system's or network's functionality, confidentiality, and honesty, as well as its performance, without jeopardizing protection.

1.11 PRINCIPLES OF CYBER SECURITY (PRINCIPLES FORMING THE BASE FOR CYBERSECURITY)

Any basic yet useful guidelines should be adopted to ensure the three essential priorities of cyber security, namely availability, confidentiality, and integrity.[50]

1. Prioritize Prior Devices: Stabilizing the degree of availability, anonymity, and dignity of services is one of the most difficult tasks, and it is accomplished by concentrating on the most important systems and ensuring the highest security cover for them, whereas other approaches are used to secure less important systems.

[48]Kurzweil, R. (2005). The Singularity is near. Penguin Group.
[49]Russell, S. J., &Norvig, P. (2000). Artificial Intelligence: A Modern Approach. Prentice Hall.
[50]Preda, M. D., Christodorescu, M., Jha, S., &Debray, S. (2008). A Semantics-Based Approach to Malware Detection. ACM Transactions on Programming Languages and Systems, 30(5), 1–54. doi:10.1145/1387673.1387674

2. Different Users, Different Levels of Accessibility: Who has access to what data can be determined by the class of user, and no one person can have complete access to all data and knowledge. This ensures that a specific duty has the bare minimum of rights. As a result, changes in rights are proportional to changes in obligation.[51]

3. Independent Protection (Protocols): Using multiple authentication protocols for a single job is much easier than using only one. It greatly decreases the probability of effective cyber-attacks, and the basic idea is to make the perpetrator work harder by requiring him to perform several actions in order to get through several layers of defenses.

4. Backups: Failures can happen, but preparing for the repercussions can help minimize the severity of the damage to the system, network, or person. This is a particularly versatile technique that is used in a variety of areas.

Keeping track of all breaches: Cyber security personnel should keep track of all breaches, which should be studied and safety mechanisms developed on a regular basis. Since hackers aren't waiting, this phase can move quickly. They're honing their talents and refining their cyber-attack tools (Panimalar, A., Giri, P.U. & Khan, S., 2018).

1.12 LET'S SUM UP

We studied basic artificial intelligence strategies that are promising in this chapter. It looked at how such methods could be used in cyber defense. We have spoke about the future of artificial intelligence and cyber defense.

1.13FURTHER READING

- Lunt, T. F., &Jagannathan, R. (1988). An example amount of your time Intrusion Detection accomplished System. Proceedings of IEEE conference on Security and Privacy.
- Nappo, S. (2017). Goodreads. Retrieved from https://www.goodreads.com Panimalar, A., Giri, P.U. & Khan, S. (2018). Artificial Intelligence Techniques

[51]Yu, W., Zhang, N., Fu, X., & Zhao, W. (2010). Self-Disciplinary Worms and Countermeasures: Modeling and Analysis. IEEE Transactions on Parallel and Distributed Systems, 21(10), 1501–1514. doi:10.1109/TPDS.2009.161

in Cyber Security. International Research Journal of Engineering and Technology, 5(3).

- Preda, M. D., Christodorescu, M., Jha, S., &Debray, S. (2008). A Semantics-Based Approach to Malware Detection. ACM Transactions on Programming Languages and Systems, 30(5), 1–54. doi:10.1145/1387673.1387674
- Russell, S. J., &Norvig, P. (2000). Artificial Intelligence: A Modern Approach. Prentice Hall. Salvador, P., Nogueira, A., França, U., &Valadas, R. (2009).
- Framework for Zombie Detection Using Neural Networks. Proceedings of The Fourth International Conference on Internet Monitoring and Protection ICIMP. 10.1109/ICIMP.2009.10

1.14CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is machine learning?**

"Machine learning is a branch of computer science that enables a computer to learn without being directly programmed." This concisely expresses the central concept. Unlike previous methods that attempted to specify a large number of laws in order to gain information from data, machine learning creates systems that learn certain rules from the data themselves.

2. **What is cyber security?**

Cyber security refers to a collection of steps and strategies for defending interconnected networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage). Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure.

1.15 ACTIVITY

Explain machine learning and types of supervisions under artificial intelligence. (Word count 2000 to 2500)

Unit 2: ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: OPPORTUNITIES AND CHALLENGES

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 AI-Human interfaces

2.4 Trustworthy AI decision making

2.5 Detection and mitigation of adversarial inputs

2.6 Let's sum up

2.7 Further reading

2.8 Check your progress: Possible Answers

2.9 Activity

2.1 LEARNING OBJECTIVES

In this chapter, we will learn-

- About human-Artificial Intelligence interactions
- AI decision making and its detection

2.2 INTRODUCTION

Recent Artificial Intelligence (AI) breakthroughs are game-changing, and they still outperform humans in tasks like visual detection, natural language processing, and data analytics. Economic dynamics will accelerate the introduction of new AI technologies that will disrupt nearly every area of business, both positively and negatively. Artificial intelligence technologies can be abused, evaded, and misled, posing serious security risks for devices such as network management software, financial systems, and self-driving cars. As a result, strategies and best practices that are safe and resilient are critical.[52]

Just as AI programs need novel cyber security techniques and approaches to enhance their trustworthiness and resiliency, cyber security will benefit from AI by increasing understanding, responding in real time, and improving overall effectiveness. This involves self-adaptation and modification in the face of continuing threats that change the existing attacker-defender imbalances. Strategies that use AI to categorize different types of attacks and notify adaptive solutions (e.g., spot anomalies easily and know how to repair them) at scale can use AI to recognise an adversary's vulnerabilities, use observation techniques, and gather lessons learned. It is well known that a small group of skilled cyber defenders can successfully secure networks that are used by tens of thousands of people. AI could apply the same degree of device security, making it universal and providing the domain information required to solve issues like quality-of-service restrictions and system failure behaviors.

[52]Cloud adoption risk report 2019 (pdf). https://mscdss.ds.unipi.gr/wp-content/uploads/2018/10/Cloud-Adoption-Risk-Report-2019.pdf (2019).

2.3HUMAN-AI INTERFACES

As threats become more complicated and serious, collaboration between AI-based cyber security systems becomes more relevant, as does coordination and trust between human-AI interfaces. Specific system elements optimize their own targets without considering system-level priorities, which causes challenges with everything from business IT to self-driving vehicles.[53] Attackers can make a module behave in a way that is ideal locally but pathological globally. Furthermore, in an age where facts can be misinterpreted, misattributed, or distorted, effective decision-making necessitates hybrid methods that combine and orchestrate human and AI capacities and viewpoints.[54]Three relevant research areas to include human-machine collaboration, fostering trust in systems and people, and delivering decision-making assistance. Human-machine collaboration must be structured in such a way that humans can comprehend, trust, and explain the results. Users must be taught how to have priorities, input, and well-formatted and meaningful data, as well as how to understand their role in the decision-making process. Human integration research is required to optimize results while minimizing latency and negative effects. To give time for human decision-making, AI is often used to automatically shut down suspicious activity.

Will this also be the case when AI is introduced to vital infrastructure like the electrical power grid, where even a brief outage could be exceedingly widespread, destructive, or dangerous? Slowing AI mechanisms to handle humans in the loop is one solution. While this would limit mobility, it would empower humans to interfere and repair failed parts. Interactions between humans and AI systems must be handled with the intention of reducing human error, increasing protection, and providing oversight in a complex human-AI system world. Adopters and users of AI systems must consider and trust the system's function.[55]

Humans must be able to recognize a system's state and forecast its behaviour under different conditions in order to have the appropriate degree of confidence.

[53]Ai in cyber security-capgemini worldwide. https://www.capgemini.com/news/ai-in-cyber security/ (2020).
[54]Ai index 2019 report (pdf). https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf(2020).
[55]Congnigo-infosecurity magazine. https://www.infosecurity-magazine.com/directory/cognigo/ (2019).

Overtrust can lead to a refusal to override a misbehaving system, while undertrust can lead to the abandonment of a system that is otherwise reliable. Human-readable, rule-based requirements based on approximating device behaviour, as well as consideration of cognitive and other biases, are needed for determining the appropriate degree of confidence. AI systems can produce incredibly persuasive false video and audio that humans can believe, according to research. Decision-making aid, such as teaching human operators to survive data falsification attacks, and AI-models that can anticipate failure modes and adjust as humans make incorrect decisions, must be included in research.

2.4TRUSTWORTHY AI DECISION MAKING

When AI systems are implemented in high-value environments, it's critical to ensure that the decision-making mechanism is reliable, particularly in adversarial scenarios. Although there are various examples of ML flaws, science-based methods for predicting trustworthiness remain elusive. Methods and concepts for a broad range of AI programs, including machine learning, planning, inference, and information representation, need research. Defining success indicators, designing methods, keeping AI programs explainable and accountable, strengthening domain-specific teaching and thinking, and handling training data are all areas that need to be discussed for trustworthy decision making.[56]To integrate robustness, anonymity, and fairness into decision-making algorithms, threat model research must recognise observable properties that determine trustworthiness.

To attain these trustworthiness properties, the device would have to reason about adversarial intervention and identify requisite criteria based on a particular threat model. Adapting cryptography or computer security concepts, unifying properties into a single logic system, and considering them as variations of a single notion of (in)stability in ML and AI for both decision making and security models more generally are both possibilities. Methods for understanding the learned reasoning of AI methods, especially deep learning, are also in need of research. What impact do those data points have on the optimization and reasoning procedures used in

[56]Knowledge-directed artificial intelligence reasoning over schemas (kairos). https://www.darpa.mil/program/knowledge-directed-artificial-intelligence-reasoning-over-schemas (2020).

machine learning systems? Analysis of the optimization process or the AI system effect, whether it captures both the training data and the learning form, are both possibilities. Techniques for estimating the effect of a training point on individual predictions may be used to determine a model's validity in a decision context. In machine learning, there are new methods that use a range of strategies to include decision assurances (e.g., convex relaxation of the adversarial optimization problem and randomized smoothing).

However, the techniques are almost entirely based on supervised learning at the moment, which is difficult to do without compromising machine efficiency. AI systems that require advice when they are unsure, a related field of study, will increase confidence in the final decision and help the system to gain knowledge for future decision making. AI's precision is also domain-specific. When training data is not indicative of the specified context, security vulnerabilities occur. In contrast, if application domain restrictions are not taken into account, excessively pessimistic risk tests will occur. Within domain-specific AI ecosystems, as well as as they become a part of the full-use ecosystem, further research is required on how input data is acquired, secured, preserved, and evaluated. An autonomous vehicle system is trained with photographs and circumstances gathered from real-world scenarios and is kept up to date as its surroundings alter. Domain-specific vulnerabilities must be recognized in perception, planning, reinforcement learning, information representation, and reasoning.

2.5DETECTION AND MITIGATION OF ADVERSARIAL INPUTS

Though AI excels at many tasks, it is susceptible to erroneous inputs that cause learning, reasoning, and planning processes to yield incorrect results. Limited quantities of feedback noise crafted by an opponent have been shown to fool deep learning methods in the past. As a result of these technologies, adversaries can monitor networks without fear of being detected.[57]If deep learning and other machine learning and AI algorithms becoming more embedded into operating

[57]Darpa robotics challenge (DRC) using human-machine teamwork to perform disasterresponse with a humanoid robot. https://apps.dtic.mil/docs/citations/AD1027886 (2020).

frameworks, it is important to consider more rigorous machine learning approaches, AI reconnaissance prevention, the analysis of adversarial models, model poisoning prevention, safe testing protocols, data protection, and model fairness to protect against adversarial inputs. Efforts to harden learning methods against adversarial inputs are needed. Both the statistical and technical community are aware of the problem. To make the same advancements in deep learning and modern ML methods without losing efficiency or precision, both theoretical and empirical research is needed.

Modern AI systems are vulnerable to reconnaissance attacks, in which adversaries challenge the systems and learn about the internal decision reasoning, information bases, and training data. This is often a precursor to an attack aimed at extracting security-relevant training data and references or obtaining the AI's intellectual property.[58] The following are some potential reconnaissance mitigation steps that should be investigated further:

- By inverting the model, you will increase the attacker's workload while lowering their efficacy.
- Use encryption techniques such as rate restricting, access controls, and deception.
- Study the effects of algorithms and processes on precision and other factors.
- Create algorithms and methods that are vulnerable to reconnaissance.
- Incorporate opposition into optimizations for learning and reasoning.
- Using modern multistep methods, embed security protections into the model.
- Using the cyber security honeypot4 model, reveal the attacker's existence and objectives. The adversary's expertise and skills identify an AI system's weakness.

To identify the various types of attacks and build effective defenses, further research is needed. Attacks must be addressed according to the kind of information that the perpetrator has access to. These models should be carefully mapped,

[58]Aljurayban NS, Emam A (2015) Framework for cloud intrusion detection system service. In: 2015 2nd world symposium on web applications and networking (WSWAN), pp 1–5

attack and protection tactics should be established, and particular research attention should be paid to security-critical environments where ML models are most vulnerable. (For example, self-driving cars and malware detection).

From training results, AI and machine learning models learn how to classify predicted inputs. The model outputs would be inconsistent if the training instances do not reflect both possible and potential scenarios. As a result, an attacker will manipulate the model and implement a loophole that can be exploited. And if an opponent only controls a portion of the training sample, the model's behaviour may be influenced (model poisoning). ML needs as much data as possible, and using multiple data sources is popular, but dangerous. The entire paradigm becomes untrustworthy if any one source of data is malicious.[59]AI best practices must guarantee the end-to-end provenance of training data and the identification of data that comes beyond the usual input space to help prevent adversarial poisoning and enhance training processes.

When used on identical data to what they were educated on, machine learning techniques perform well, but when the data is new, they struggle (e.g., a self-driving car trained in sunny, cloudy, rainy, and snowy weather might operate poorly in sleet or hail). There are general issues since gathering data for all potential scenarios is difficult. And where a person does, systems normally do not detect suspicious data. The aim of the study is to improve anomaly identification, implement training methods that intensify unusual events, and make the best use of existing training data and algorithms.ML models must be retrained on a regular basis to stay successful and reliable (e.g., social media terminology used for public sentiment analysis changes over time as vocabulary and topics of interest change). To determine what training data to obtain, when such training data is no longer valid, and how much models should be retrained, further research is needed. An adversary can decide if a data item was used in training a model, according to recent attacks. Many applications necessitate ML training for private data, putting personal data at risk.

More research is required, but advancements like differential privacy open up new

[59]Bao H, He H, Liu Z, Liu Z (2019) Research on information security situation awareness system based on big data and artificial intelligence technology. In: 2019 international conference on robots intelligent system (ICRIS), pp 318–322

avenues for anonymizing data and preventing leaks. Finally, models can pick up on any prejudices and biased characteristics in the training results. If the evidence shows prejudice towards a certain population (for example, in college enrollment or loan approvals), the result would show that bias. The development of scientific and technological foundations for ML justice would be needed to prevent outcome bias. To quantify, identify, and diagnose unequal ML training data and procedures, goals must be established and algorithmic techniques built.

2.6 LET'S SUM UP

We studied basic artificial intelligence techniques and the principle of machine learning in this chapter. We have also figured out how humans and AI communicate and how it affects cyber rules.

2.7FURTHER READING

- Johnson, J. (2014). Remarks by Secretary of Homeland Security Jeh Johnson at the White House Cyber security Framework Event. Retrieved from https://www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cyber security-framework
- Jonze, S. (2017). 28 Best Quotes about Artificial Intelligence. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/07/25/28-best-quotes-about-artificial-intelligence
- Kivimaa, J., Ojamaa, A., &Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. Proceedings of Military communications conference, MILCOM 2008.
- Kivimaa, J., Ojamaa, A., &Tyugu, E. (2009). Graded Security accomplished System. In Lecture Notes in engineering (Vol. 5508, pp. 279–286). Springer.
- Kurzweil, R. (2005). The Singularity is near. Penguin Group.

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

What is cyber security?

Cyber security refers to a collection of steps and strategies for defending

interconnected networks, applications, hardware, and data from cyber-attacks (unauthorized access and damage). Where it comes to computers, both cyberspace and physical space security are equally essential. Cyber security includes components such as application security, information security, network security, organizational security, and others that function together to secure the whole information infrastructure.

How does cyber security benefit from AI?

Just as AI programs need novel cyber security techniques and approaches to enhance their trustworthiness and resiliency, cyber security will benefit from AI by increasing understanding, responding in real time, and improving overall effectiveness. This involves self-adaptation and modification in the face of continuing threats that change the existing attacker-defender imbalances. Strategies that use AI to categorize different types of attacks and notify adaptive solutions (e.g., spot anomalies easily and know how to repair them) at scale can use AI to recognise an adversary's vulnerabilities, use observation techniques, and gather lessons learned. It is well known that a small group of skilled cyber defenders can successfully secure networks that are used by tens of thousands of people.

2.9 ACTIVITY

Explain AI decision-making process and AI- human interaction. (Word count 2000 to 2500)

Unit 3: ARTIFICIAL INTELLIGENCE POLICY IN INDIA: A FRAMEWORK FOR ENGAGING THE LIMITS OF DATA-DRIVEN DECISION-MAKING

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Scope

3.4 India's policy landscape

3.5 NITI Aayog National Strategy

3.6 Let's sum up

3.7 Further reading

3.8 Check your progress: Possible Answers

3.9 Activity

3.1 LEARNING OBJECTIVE

In this chapter, we will learn-

- Policy making for Artificial intelligence
- AI related concepts like machine learning and process involved in AI decision-making.
- NITI aayog strategy for Artificial intelligence.

3.2 INTRODUCTION

The word Artificial Intelligence (AI) remains in vogue more than half a century since it was coined. Artificial intelligence determines the content we consume on social media, determines risk judgments of offenders in criminal sentencing, determines credit-worthiness of people, and also suggests the best path home from work. Most AI systems are trained on historical data and are capable of detecting trends, learning from examples, and forecasting potential outcomes for decision-making purposes. This generalizations are focused on massive databases that humans will be unable to interpret at the same speed and size.[60]AI's effect is thought to be so revolutionary that it has been dubbed the "new electricity." The social and ethical ramifications of these innovations have come into view as industry and policymakers work to evolve and apply them.

Since the Indian government places a high priority on new technology in the digital economy, AI strategy will change and grow quickly in the coming years. Aadhaar, the world's largest biometric identification initiative, is located in the country and, depending on how it is used, will serve as a focal point for AI applications. India is also at a crucial juncture in the implementation of data security legislation, which will have a significant impact on how AI can and can work in the country.

Although the introduction addresses the issue that this article aims to solve, the next section will go over the chapter's intended scope and include definitions and

[60]Balkin J. 2017 Free speech in the algorithmic society: big data, private governance, and new school speech regulation. U.C. Davis L. Review, Forthcoming 2018. See https://papers.ssrn. com/sol3/paperscfm?abstract_id=3038939.

logical clarifications for technical terms used in the chapter.[61] It will address the current state of India's AI policy environment before taking the reader through each stage of the framework, with the aim of providing theoretical history for thinking through the proposed framework. Finally, this approach is applied to industries that are actually being discussed by India's policymakers. Conclusions and reflections will be used at the end of the chapter.[62]

3.3SCOPE

The word "AI" can be interpreted in a variety of ways. Given the difficulty in defining terminology in this field, I explain a few technical terms in this section and describe their intended reach within the context of this article. - A collection of "encoded procedures for converting input data into desired results, based on precise formulas" is referred to as an algorithm. It's a methodical, step-by-step process that doesn't rely on human instincts or guesswork.[63]

Artificial intelligence refers to a computer's ability to behave intelligently. There are three forms of AI. The first is artificial superintelligence, which is the concept that machines can outperform humans in terms of intelligence, social abilities, and scientific expertise in a variety of realms. Artificial general intelligence is the second. This applies to the target of machines displaying knowledge in many contexts, if not on par with human intelligence. Any of these AI types are both technically conceivable and completely implausible, according to some researchers.The third kind is artificial narrow intelligence (ANI), which refers to computers' ability to mimic human skills in specific, intentional domains. The word AI will be used to refer to ANI alone for the purposes of this paper.

Machine learning (ML) is the most effective and widely used branch of AI strategies today, demonstrating a system's ability to increase task efficiency over time. Today, much of what is referred to as "AI" is simply machine learning. Machine learning algorithms, according to Arthur Samuel, have the ability to learn without being directly coded. In order to increase efficiency on future assignments, machine

[61]Angwin J, Larson J, Mattu S, Kirchner L. 2016 Machine Bias. ProPublica. See https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[62]O'Neil C. 2016 Weapons of math destruction: how big data increases inequality and threatens democracy, pp. 278–315. New York, NY: Crown Publishing Group.
[63]O'Neil C. 2016 Weapons of math destruction: how big data increases inequality and threatens democracy, pp. 278–315. New York, NY: Crown Publishing Group.

learning relies on results. Existing research has demonstrated that data bias can result in overwhelmingly negative results, further entrenching societal prejudice.

The majority of machine learning applications rely on data. Developers of machine learning systems use training data to train variations of these algorithms. The paradigm evolves as a result of the preparation. Machine learning is an iterative technique, which entails a continuous process of analyzing these models and adapting training data and learning algorithms to optimize for performance, as described and decided by developers.

Machine-learning strategies, as previously said, depend for instructions on what to look for. Feature engineering, or choosing the characteristics the machine-learning algorithm can train, is an important human factor in machine learning.[64] In reality, this is a much more difficult job for developers than actually performing the learning process. Although attempts to minimize human interference in feature selection are growing, this is impossible.[65]

3.4 INDIA'S AI POLICY LANDSCAPE

The Indian government has placed AI growth, adoption, and promotion at the top of its priority list, based on the belief that AI has the ability to make people's lives simpler and society more equitable.[66] The Union government dedicated significant funds to research, training, and skilling in new technologies such as AI in 2018, an expansion of 100 percent over previous investments. This focus on emerging media is nothing new. The Digital India initiative of the Union government aims to turn India into a "digitally driven society and information economy."Digital India aspires to make digital technology a central utility for all people, integrating such digitisation into government, and eventually empowering citizens.

The Digital India initiative is responsible for increasing support for testing, training, and skilling in new technologies such as artificial intelligence. The government has also started working to ensure that AI technology is made in India and designed to benefit India, as part of its Make In India project, which aims to promote India as a

[64]Elish MC, Hwang T. 2016 An AI Pattern Language, Intelligence and Autonomy initiative (I&A) at Data & Society. See https://www.datasociety.net/pubs/ia/AI_Pattern_Language.pdf.
[65]Domingos P. 2012 A few useful things to know about machine learning. Commun. ACM 55, 78–87.
[66]Gillespie T. 2014 The relevance of algorithms, Media technologies: essays on communication, materiality and society 167.

global manufacturing hub. Though AI has been a major concern in emerging technology in general, a variety of AI-specific initiatives have also arisen.

3.5NITI AAYOG'S NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE: #AIFORALL

A government-run think tank, the National Institution for Transforming India (also known as NITI Aayog), has been charged with developing a national artificial intelligence strategy to guide the government's AI efforts. In early May 2018, NITI Aayog partnered with Google to train and incubate startups looking to build and embed AI-based technologies into their business models in an attempt to improve economic productivity in India. In late May 2018, NITI Aayog and ABB India signed a letter of intent to 'make core sectors of the Indian economy ready for a digitalized future and recognize the promise of AI, big data, and connectivity.'[67]

NITI Aayog's ultimate target for a national AI strategy is to "leverage AI for economic growth, social change, and sustainable growth, and finally as a "Garage" for emerging and developed economies," according to a discussion paper published in June 2018. The task of the NITI Aayog goes beyond simply proposing a policy approach; it also involves execution and deployment. In two aspects, the National Strategy goes beyond and above any other AI policy mechanism.[68] First, it admits that AI implementation has primarily been motivated by business interests to date, and it recognizes the "need to find a balance between limited financial effects concepts and the common good."Second, it recognizes that AI implementations in different sectors should be accepted for their incremental benefit rather than their alleged transformational value.[69]

Among these positive changes in outlook, India's national policy on AI's practical advice and review leave a lot to be desired. Education, agriculture, healthcare, smart cities & infrastructure, and smart mobility & transportation are the five primary sectors where AI may have a positive social impact and require the government to

[67]NITI Aayog. 2018 National strategy for artificial intelligence. NitiAayog 46. See http://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AIDiscussion-Paper.pdf.
[68]Make 'Artificial Intelligence' work for India: PM. The Economic Times. See https://cio.economictimes.indiatimes.com/news/government-policy/make-artificial-intelligence-work-forindia-pm/62980259.
[69]Gupta K. 2018 NitiAayog partners with Google to grow India's artificial intelligence ecosystem. Livemint. See https://www.livemint.com/Industry/fpnGnNQ8duTCRZOEpk 2P6M/Niti-Aayog-partners-with-Google-to-grow-Indias-artificial-i.html.

play a leading role, according to the study. The study advocates the use of AI for security purposes when addressing smart cities.AI devices that forecast crowd behaviour that can be used for crowd control, “sophisticated monitoring systems” that can monitor people’s activity and behavior, and social media intelligence networks that can help with public safety are among them.[70]

The report’s guidelines in the form of smart cities did not mention the major shortcomings of consistency and justice, as well as the negative effects of surveillance on fundamental rights. This is particularly concerning because India’s surveillance system currently lacks sufficient protections to protect against law enforcement agencies’ possible erosion of fundamental freedoms. As a result, AI-assisted monitoring should be the exception rather than the rule. The study acknowledges that bias is rooted in evidence, with the likelihood of such bias being compounded over time, when addressing justice in AI systems as an issue.

One potential solution is to “identify the in-built biases and determine their effect, and then find ways to reduce the bias,” according to the study. When the fact is that skewed evidence comes from a biased, unjust, unjust, and oppressive society, it takes a ceteris-paribus approach, i.e. all other factors are similar, merely defining and mitigating prejudice in datasets will expect to achieve fairer outcomes. This method has a flaw in that it only considers AI as a statistical construct, rather than as a socio-technical structure. Understanding and adapting to the social context in which these programs will operate is critical to reducing prejudice within them.Indeed, avoiding discriminatory consequences should be the aim. As Eubanks points out, unless automatic decision-making tools are designed to address socioeconomic inequities, their use would exacerbate them.[71]

3.6 LET’S SUM UP

Learned about the context of India’s existing AI policy environment, as well as the proposed roadmap for addressing India’s ongoing sectoral challenges. We learned about the possible dangers of data-driven decisions in general, and in the Indian context in particular, in order to influence current policy debates in the region.

[70]Sharma YS, Agarwal S. 2018 NitiAayog to come out with national policy on artificial intelligence soon. The Economic Times. See https://economictimes.indiatimes.com/news/ economy/policy/niti-aayog-to-come-out-with-national-policy-on-artificial-intelligencesoon/articleshow/63387764.cms.
[71]Artificial Intelligence Task Force. See https://www.aitf.org.in/.

3.7FURTHER READING

- Elish, M.C. 2016 Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. We Robot 2016 Working Paper. (DOI: 10.2139/ssrn.2757236)India Stack. Available from http://indiastack.org/about/.
- Sainath, P. 2018 In India, Farmer's Face a Terrifying Crisis. The New York Times. Available from https://www.nytimes.com/2018/04/13/opinion/india-farmers-crisis.html.
- Eckerslet, P., & Cohn, C. 2018 Google Should Not Help the U.S. Military Build Unaccountable AI Systems. Electronic Frontier Foundation. Available from https://www.eff.org/deeplinks/2018/04/should-google-really-be-helping-us-military-build-aisystems.
- RakshaMantri Inaugurates Workshop on AI in National Security and Defence. Press Information Bureau, Government of India. Available from http://pib.nic.in/newsite/PrintRelease.aspx?relid=179445.

3.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is artificial intelligence?**

Artificial intelligence refers to a computer's ability to behave intelligently. There are three forms of AI. The first is artificial superintelligence, which is the concept that machines can outperform humans in terms of intelligence, social abilities, and scientific expertise in a variety of realms.

2. **What is machine learning?**

Machine learning (ML) is the most effective and widely used branch of AI strategies today, demonstrating a system's ability to increase task efficiency over time. Today, much of what is referred to as "AI" is simply machine learning. Machine learning algorithms, according to Arthur Samuel, have the ability to learn without being directly coded.

3.9 ACTIVITY

Explain NITI Ayog strategy for artificial intelligence. (Word count 2000 to 2500)

Unit 4: PROSPECTS OF ARTIFICIAL INTELLIGENCE IN TACKLING CYBER CRIMES

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Cyber Crimes

4.4 Artificial Intelligence

4.5 Intrusion Detection and Prevention System

4.6 Applications of AI Techniques in Defending Cyber Crimes

4.6.1 Application of Artificial Neural Networks against Cyber Crimes

4.6.2 Application of Intelligent Agents against Cyber Crimes

4.7 AI flexible features for IDPSs

4.8 Limitations of Existing Anomaly Detection and Prevention System

4.9 Let's sum up

4.10 Further reading

4.11 Check your progress: Possible Answers

4.12 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- What Artificial Intelligence is in a broader manner
- AI's role in the protection of cyber crimes
- How AI applications can defend cyber crimes

4.2 INTRODUCTION

Since we live in an interactive online environment, we now use the Internet for the majority of our daily interactions and commercial activities. Rising internet computing developments pose concerns about cyberspace information security. Threats and intrusions exist in cyberspace. People, companies, and governments are all targets of cyber-threats that travel at the speed of light. It is self-evident that the best way to defend against intelligent cyber devices is to use intelligent applications. Because of the high speed of cyber operation and the vast amount of data involved, cyberspace security cannot be done only by physical devices or human interaction.[72] To identify threats and make intelligent real-time decisions, it needs a significant amount of automation. It's difficult to create applications that efficiently protects against rapidly changing threats using traditional algorithms. This is why we need novel techniques, such as using Artificial Intelligence (AI) methods to help humans combat cybercrime by providing machines with versatility and learning capabilities.

4.3 CYBER CRIMES

Cybercrime is on the rise in tandem with the expansion of the Internet. Internet crime has multiple faces and is perpetrated in a variety of ways. The term "cybercrime" refers to criminal acts carried out using computers and the internet. Cybercrime is fueled by the evolution of the internet and its global diversity.[73] Cybercrime can be divided into two distinct groups. One of them considers the network to be a criminal object, such as interference, network system destruction, and so on. The rest are people who use the internet to commit crimes like theft.

While the term "cybercrime" has been widely used, it is difficult to describe precisely. "Cybercrime is a term used commonly to describe illegal activity in which computers or computer networks are a weapon, a target, or a location of criminal activity," according to Somaiya et al. (2014).[74] "Offenses perpetrated against individuals or groups of people with a criminal purpose to deliberately damage the victim's reputation or inflict physical or mental harm, or failure, to the victim directly or indirectly, using electronic telecommunication networks such as the Internet and cell

[72]Selma Dilek, HüseyinÇakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015

[73]Manveer Kaur, ShevetaVashisht, Kumar Saurabhi, "Adaptive Algorithm for Cyber Crime Detection", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012

[74]JheelSomaiya, DhavalSanghavi, ChetashriBhadane, "A Survey: Web based Cyber Crimes and Prevention Techniques", International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014

phones," according to Halder et al (2011).Cybercrime, according to Kandpal et al (2013), "requires all unauthorized access to information and breaches of security such as anonymity, passwords, and so on through the use of the internet." Virus assaults, financial crimes, the selling of illegal articles, pornography, internet gaming, e-mail spamming, cyber phishing, cyber harassment, unlawful access to computer systems, stealing of information stored in electronic form, e-mail bombing, physically destroying computer systems, and so on are all examples of cybercrimes.[75]
The numbers that have been gathered and reported on show how widespread Internet crimes are around the world. Phishing emails alone bring in one billion dollars for the criminals who send them. In a survey conducted by the FBI in early 2004, 90 percent of the 500 businesses surveyed said they had experienced a security breach, with 80 percent of those saying they had suffered a financial loss.[76] According to a nationwide estimate from 2003, four billion dollars were spent per year due to credit card theft. Just 2% of credit card transactions are done over the Internet, but they account for half of the four billion transactions listed earlier.Many of these findings serve as examples of how the Internet is being abused and that Internet violence must be curtailed.

4.4ARTIFICIAL INTELLIGENCE

In July 1956, at Dartmouth College's Summer Science Project, AI (then known as machine intelligence) became a research discipline. The concept was coined by John McCarthy, who describes it as "the science and engineering of creating intelligent machines." "Artificial Intelligence is the exploration of how to make machines do stuff that humans do better at the moment," according to a widely agreed description.[77] Reasoning, information, organizing, listening, natural language processing (communication), vision, and the capacity to move and control objects are all key problems (or goals) in AI science. Three capabilities are required of an AI system.
i. Save information;
ii. Use the information to fix problems
iii. Gain new skills by practice.
Representation, Reasoning, and Learning are the three main components of AI.[78]
The challenge of simulating intelligence has been broken down into smaller sub-problems, each of which has unique features or attributes that an intelligent machine should have. The following characteristics have received the most attention:

a) Deduction, reasoning, problem solving
b) Knowledge representation
c) Planning
d) Machine learning
e) Natural Language Processing

[75]Halder, D. Jaishankar, K, "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations". Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[76]VineetKandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013
[77]V. Rajaraman, "John McCarthy – Father of Artificial Intelligence", in General Article Resonance, March 2014
[78]T N Shankar, Neural Networks, LAXMI Publications Pvt. Ltd, 2008

f) Motion and Manipulation

g) Perception

h) Social Intelligence

i) Creativity

j) General Intelligence

Individual human actions, information interpretation, and inference techniques are the core focuses of traditional AI approaches. Distributed Artificial Intelligence (DAI), on the other hand, is mostly concerned with social activity. DAI systems are cooperative systems in which a group of agents works together to solve a problem. These agents are often diverse. “An agent may be a real or virtual being that can function, interpret its environment (in a partial way), interact with others, is autonomous, and has skills to accomplish its aims and tendencies,” writes Jacques Ferber (1999).[79]Agents are discrete entities with specified borders and interfaces that are used to solve problems. A multi-agent scheme, on the other hand, is a loosely connected network of agents that function as a single unit, similar to a society, to solve problems that an independent agent cannot. The following are the major implementations of multi-agent systems:

- Problem Solving
- Multi-Agent Simulation
- Synthetic World Construction
- Collective Robotics
- Kenetic Program Design

Computational Intelligence (CI) is a branch of AI that focuses on heuristic algorithms including fuzzy systems, neural networks, and evolutionary computation. The terms “Soft Computing” and “Computational Intelligence” are synonymous. Computational Intelligence has recently expanded to include new fields such as artificial immune systems, swarm intelligence, chaotic systems, and so on. Neural networks, fuzzy logic, evolutionary computation, swarm intelligence, deep learning, and artificial immune systems are examples of nature-inspired approaches that offer versatile decision-making mechanisms for problems like cyber security.[80]
Another kind of AI technique is genetic algorithms. Also for complex computing problems, they have reliable, scalable, and optimal solutions. They can be used in intrusion detection systems to generate guidelines for classification of security attacks and to create new rules for various security attacks (IDS).

4.5INTRUSION DETECTION AND PREVENTION SYSTEM

Where traffic does not pass through the firewall at all, an Intrusion Detection System (IDS) can provide protection against external users and internal attackers. The

[79]J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003

[80]Jacques Ferber, Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman, 1999

firewall protects an organisation against disruptive Internet threats, and the IDS detects whether anyone attempts to hack through the firewall or manages to break through the firewall protections to gain access to some device on the trustworthy hand. If there is a security violation, it notifies the system administrator. An IDS is similar to a smoke detector in that it can sound a warning if such conditions are met.[81]

An Intrusion Detection System (IDS) is a computer or piece of software that tracks network or system activity for malicious activity or policy breaches and sends notifications to a management station. Network-based Intrusion Detection Systems (NIDS) and host-based Intrusion Detection Systems (HIDS) are two types of IDS (HIDS).

IDS executes a number of tasks, including:

- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity by statistical analysis
- Managing audit trials and highlighting user policy violations or normal activity

An intrusion detection and prevention system (IDPS) is a software or hardware unit that is installed within a network that can detect and avoid intrusions.[82]

When compared to conventional approaches, Artificial Neural Networks (ANNs) can improve the efficiency of Intrusion Detection Systems (IDS). In the search for artificial intelligence, artificial neural networks are a turning stone. ANNs are information retrieval systems that are modeled after the biological nervous system. We can build AI using the tools provided by ANN.

4.6APPLICATIONS OF AI TECHNIQUES IN DEFENDING CYBER CRIMES

AI methods have a wide range of uses in cybercrime identification and mitigation, according to scholarly resources. For example, neural networks may be used to create a highly effective intrusion detection and prevention method. There is also a proposal for using artificial neural networks in the analysis of DoS attacks, computer worms, spam, and zombies, as well as malware recognition and forensic examination.[83] To increase their performance, next generation antivirus programs employ AI techniques such as data mining, neural networks, and heuristics approaches. Intelligent agents and mobile agents are also used in distributed wireless intrusion detection systems (IDS). IDS focused on mobile agents offer

[81]N. A. Alrajeh and J. Lloret," Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol.2013, Article ID 351047.

[82]S. Shamshirband, N. B. Anuar, M. L. M. Kiah, A. Patel, "An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique," Engineering Applications of Artificial Intelligence, Vo. 26, pp. 2105–2127

[83]X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, "Review on the application of Artificial Intelligence in Antivirus Detection System", In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506-509,2008

network protection by incorporating accessibility capabilities into the detection of malicious cyber behavior.

4.6.1APPLICATION OF ARTIFICIAL NEURAL NETWORKS AGAINST CYBER CRIMES

An Artificial Neural Network (ANN) is a massively parallel distributed processor made up of basic processing units that has a built-in capability for storing and retrieving experimental information. Chen (2008) presented NeuroNet, a neural network device capable of tracking flow, detecting traffic disturbances, and initiating countermeasures. NeuroNet is successful against one form of secret attack known as low-rate TCP targeted distributed DoS attacks, also known as shrew attacks, according to the findings of the NS-2 experiment.[84]

Iftikhar et al. (2009) developed an ANN-based method for detecting probing attacks. It used a supervised neural network phenomenon to test the viability of a method for probing attacks in computer network networks that are the foundation of other attacks. When the evolved framework is subjected to various probing attacks and its efficiency is compared to that of other neural network approaches, the results show that the approach based on Multiple Layered Perceptron (MLP) architecture is more detailed and reliable, and that it produces the best results when compared to other methods.

Linda et al. (2009) presented a novel IDS-NNM – Intrusion Detection System using Neural Network based Modeling – that employs a unique combination of two neural network learning algorithms for behaviour modeling, namely Error-Back Propagation and Levenberg-Marquardt. The IDS-NNM algorithm is capable of catching all intrusion attempts posed in network communication without producing any false alarms, according to experimental findings.[85]

With the aim of improved performance, Barika (2009) proposes an Artificial Neural Network architecture for decision making within intrusion detection systems.

Brij is a word that comes to mind when (2011) An ANN is used to approximate the amount of zombies involved in a flooding DDoS attack, which is useful in reducing the attack's effect.[86]

Wu (2009) proposed a spam filtering approach that combines rule-based computation and back-propagation neural networks. This technique has proved to be much more robust than other spam detection methods that consider keywords, since spamming patterns can alter frequently.[87]

Kufandirimbwa and Gotora (2012) proposed a spam filtering strategy based on Artificial Neural Networks and the perception learning process, which has higher detection rates than other spam detection methods based on text and other message characteristics due to the inclusion of a continuous learning function.

---

[84]M Rajesh Kanna, D. Hemapriya and C. Divya," Intelligent Agents For Intrusion Detection System (IAIDS)", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013. [21]N. Jaisankar, R. Saravanan, K.DuraiSwamy, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009

[85]Yu Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure", In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008

[86]BrijBhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack", International Journal of Network Security, Vol.14, PP. 61–70, Mar 2012

[87]Ondrej Linda, Todd Vollmer and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", In Proceedings of the International Joint Congress on Neural Networks, 2009

Zhai (2014) suggested a multi-agent distributed IDS (DIDS) paradigm for intrusion detection based on BP neural networks, which has the benefits of reducing the amount of mobile data processing, load balancing, neatly detecting analysis, better error-tolerating, and effectively detecting distributed intrusion.

4.6.2APPLICATION OF INTELLIGENT AGENTS AGAINST CYBER CRIMES

Intelligent agents are self-contained computer-generated forces that can interact with one another and exchange data, as well as collaborate to prepare and execute effective responses in the event of unpredictable events. Intelligent agents are well-suited to countering cyber attacks because of their versatility, adaptability in their deployment environments, and collaborative existence.

Using multiagent preparation and some innovative inference approaches, Rowe (2003) created a technique to systematically counter plan the ways to deter specific cyber attack plans.

Helano (2006) presented a Prolog-oriented architecture that is a synthesis based on a multi-agent systems (MAS) approach, with a realistic argument for fighting cyber intrusions and the potential to validate cybercrime assets.[88]

Mueen Uddin et al. (2010) introduced a modern paradigm called Dynamic Multi-Layer Signature based IDS with Mobile Agents, which can identify imminent threats with a high success rate by dynamically and automatically building and utilizing tiny and effective multiple databases, with a method to upgrade these small signature databases at frequent intervals using Mobile Agents.

To address the shortcomings of current Mobile Agent-based Intrusion Detection Systems, Onashoga et al (2013) suggested a Multi agent-based architecture for Intrusion Detection System (IDS) with three main phases: data gathering, detection, and response.

M. Rajesh Kanna et al. (2013) created a wireless distributed Wireless Intrusion Detection System (WIDS) focused on Intelligent agents with four main components: Intrusion detection module, Warning, Mobile agent platform, and Test suit.[89]

4.7AI FLEXIBLE FEATURES FOR IDPSs

AI strategies have a number of characteristics that make them ideal for building an intrusion detection and prevention scheme.

Technologies and their features:

1. Artificial Neural Networks
    i. Learning by example.
    ii. Resilience to noise and incomplete data.
    iii. Intuitiveness since it mimic biological neuron.
2. Intelligent Agents

[88]IftikharAhmad, Azeen Abdullah, and Abdullah Alghamdi, "Towards the selection of best neural network system for intrusion detection".

[89]BrijBhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack", International Journal of Network Security, Vol.14, PP. 61–70, Mar 2012

i. Mobility.
ii. Adaptability.
iii. Collaboration

3. Artificial Immune Systems
   i. Self-adaptability.
   ii. Self-organizing.
   iii. Dynamic nature
4. Genetic Algorithms and fuzzy
   i. Optimization.
   ii. Robustness.
   iii. Flexible

4.8 LIMITATIONS OF EXISTING ANOMALY DETECTION AND PREVENTION SYSTEM

IDPS have been increasingly useful in improving the reliability of networks and end hosts in recent years; however, they have a number of significant disadvantages.[90] They are as follows:

- Encryption: After data packets have been secured, current security systems can be rendered useless in detecting intrusions.
- Signature evasion: polymorphic worms that can change their propagation properties and hence their signatures automatically. These worms are also a serious threat to the existing detection scheme.
- False Positives: A false positive occurs when an intrusion detection system (IDS) incorrectly raises a security hazard warning for innocuous traffic.
- Regulatory requirements: intrusion detection devices must adhere to legal requirements.
- IDPS attack: if attackers can figure out how the device operates, they can be able to kill it.

4.9 LET'S SUM UP

Since we now live in an interconnected environment, the majority of our daily conversations and business operations are now conducted over the Internet.

[90] ZhaiShuang-can, Hu Chen-jun and Zhang Wei-ming, "Multi-Agent Distributed Intrusion Detection System Model Based on BP Neural Network", International Journal of Security and Its Applications Vol.8, pp.183- 192, 2014.

However, it has resulted in difficult-to-manage problems, such as the rise of cybercrime. Academic tools reveal that AI methods are now being used to tackle cybercrime in a variety of ways. We've briefly discussed the capabilities of AI strategies in the area of cybercrime so far, as well as their existing shortcomings.

4.10FURTHER READING

- Selma Dilek, HüseyinÇakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015.
- JheelSomaiya, DhavalSanghavi, ChetashriBhadane, "A Survey: Web based Cyber Crimes and Prevention Techniques", International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014.
- Halder, D. Jaishankar, K, "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations". Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.
- VineetKandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013.
- J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003.
- Manveer Kaur, ShevetaVashisht, Kumar Saurabhi, "Adaptive Algorithm for Cyber Crime Detection", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012.
- M Rajesh Kanna, D. Hemapriya and C. Divya," Intelligent Agents For Intrusion Detection System (IAIDS)", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013. [21]N. Jaisankar, R. Saravanan, K.DuraiSwamy, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009

4.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is an Intrusion Detection System?**

An Intrusion Detection System (IDS) is a computer or piece of software that tracks network or system activity for malicious activity or policy breaches and sends notifications to a management station.

2. **What is an Intrusion Detection and Prevention System?**

   An intrusion detection and prevention system (IDPS) is a software or hardware unit that is installed within a network that can detect and avoid intrusions.

3. **What is ANNs?**

   ANNs are information retrieval systems that are modeled after the biological nervous system.

4.12 ACTIVITY

1. Discuss about IDPS and how are they able to contribute in the prevention of cybercrimes. (400-500 words)
2. Critically analyse the AI's role in the protection of cybercrimes. (1200-1500 words)

Block-3

DATA PROTECTION AND PRIVACY

Unit 1: AI AND PRIVACY LAW

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 The Unrealized Value of Learned Intelligence

1.4 Computer Vision and AI: Who Owns the Neural Network within AI?

1.5 The Value of Learned Intelligence in the Insurance Industry

1.6 Negotiate with Understanding

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible Answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- the unrealized value of Learned Intelligence
- Artificial Intelligence and Computer Vision
- how Learned Intelligence affects the Insurance Industry

1.2 INTRODUCTION

Manufacturers and service providers are now faced with previously unconsidered ways to extract benefit through the reuse and repurpose of data originally gathered and harvested for other purposes, thanks to the exponential proliferation of technology through any area of business.[91] Artificial intelligence (AI) systems add meaning to the processor that had not previously been understood or accepted in transactions. This is especially relevant when it comes to how AI firms who partner with insurers to improve claims management are left with a valuable resource after the data is collected.

1.3THE UNREALIZED VALUE OF LEARNED INTELLIGENCE

Data protection and privacy have been hot topics in the business world, civil rights groups, and even sovereign nations over the last decade. Massive data leaks have disclosed confidential details, government hackers have revealed classified information, and internet hacks have revealed nude celebrity images and the use of discreet dating apps for extramarital affairs. The founder of Facebook was summoned to appear before Congress on the subject of privacy. The European Union and the state of California, among others, have adopted comprehensive laws to regulate people's privacy and data access.[92] Despite this, the corporate world continues to search for productivity nirvana – the use of data for specific activities. The insurance sector, which is one of the most heavily regulated sectors in terms of anonymity, has recognised the importance of data and is working to build on it. With the increased use of AI in the analysis of such data, the industry must consider a number of considerations when engaging in transactions involving such data.

People have practiced Sir Francis Bacon's theory of "scientiapotentiaest," a Latin aphorism that means "intelligence is force," for more than 400 years. Companies depend on analytics to advise their operations, managers, and strategies now more than ever to increase their market strength. The development in artificial intelligence (AI) over the last 60 years has had a huge effect on our daily lives. When one opens a Facebook newsfeed, conducts a Google search, or receives a suggestion from a well-known website, AI is at work.AI is used by consumers who use robotic vacuum cleaners or navigation software to help them find the right way. Amazon, a household name in most Americans' lives, has expanded its company largely thanks

[91]Shrikant, Ardhapurkar& Srivastava, &Tanu, & Swati, Sharma &chaurasiya, Mr &Vaish, Abhishek. (2010). Privacy and Data Protection in Cyberspace in Indian Environment. International Journal of Engineering Science and Technology. 2.

[92]Privacy-Enhancing Technologies—approaches and development http://www.sciencedirect.com/

to artificial intelligence. But, what's the big deal? AI seems to be changing our lives, with improved health services, financial management, and a better social climate on the horizon.

When AI is mixed with questions over data protection and possession, a problem emerges. We're discussing the importance of info, which has been dubbed the "fresh" oil. Clive Humby, the British mathematician behind Tesco's Clubcard rewards scheme and My Kroger Plus, is credited with coining the phrase "information as an asset, equal in worth and usefulness to gasoline."[93] Although data is intrinsically useful, it must be processed, just as oil must be refined before it can achieve its full value, according to Humby. Data is used to power transformative developments in the same way as oil has fueled industrial development. Data has many benefits, including the ability to be conveniently transported and reused at a low cost. Furthermore, unlike oil, data can become more valuable the more it is used. As a result, data is equivalent to and more useful than oil in several respects.

Having said that, the concept of data manipulation has been somewhat concrete and observable until recently. Data is created by processes, which are then siloed by departments and stored in databases or filing cabinets, or by a series of processes. This data is typically easy to locate, inspect, and monitor, especially when it is used and handled by contracts and outsourcing agreements. The data can be picked up, reused, and transferred to a new process, or it can be outsourced and reused. Customers purchasing and renewing insurance from a website, for example, may be transferred into an application with some preparation for a better or different user experience. Although the content of data has not improved, the concept of data interconnection is encouraging new applications of analytics, ranging from stock trading to professional sports. Data has a primary function, and its interrelationship with other data has a certain role.

When a motorist is involved in a car crash, the insured records information such as the model of vehicle, the injury, the site of the accident, the driver, the passenger, and the conditions, to name a few. Much of this information is used to process the collateral loss petition, as well as any possible physical injury and medical insurance claims. However, as this data is exposed to algorithms and artificial intelligence, it may be used for other purposes.[94]

If a motorist is involved in a car crash, data can theoretically be aggregated to draw some conclusions when the data is linked to other data. For instance, the type of car and the injury it sustains can be used to draw conclusions about the safety of vehicles involved in collisions, the cost of property damage, and also the risk of being involved in a "accident." The accident's location will aid in the identification of hazardous places and road conditions. The identities of the drivers and passengers, as well as the injuries they suffered, will be used to assess if cars are adequately equipped with safety features. The list continues on and on. The argument is that the information gathered isn't only helpful with the accident in question; it can even be used for a variety of different things when combined with other information. The data gathered from these analytics will be beneficial to the collector and researcher. It is

---

[93] Philip E. Agre, Marc Rotenberg Technology and privacy: the new landscape http://books.google.co.in/books?id=H2KB2DK4w78C&printsec=frontcover&dq=technology+and+privacy&source=bl&ots=1UZmu8TrQp&sig=YJJNgSU61_nTcL_CnCl7Je2LcrQ&hl=en&ei=7L2YS_T2KYSysgOygbnCAQ&sa=X&oi=book_result&ct=result&resnu m=2&ved=0CAkQ6AEwAQ#v=onepage&q=&f=false

[94] White Paper on Privacy Protection in India :Vakul Sharma http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy. %202007.pdf

valuable and referred to as “oil.” However, who owns the data and how useful it is is up for debate.

1.4COMPUTER VISION AND AI: WHO OWNS THE NEURAL NETWORK

AI technology has the potential to drastically alter industries and operations, just as the steam engine and assembly line did with production. Company sees potential benefit in the opportunity to ramp up without incurring large human costs. This untapped productivity and “knowledge capacity” is being commoditized and accepted as a valuable resource.AI technology has the potential to drastically alter industries and operations, just as the steam engine and assembly line did with production. Company sees potential benefit in the opportunity to ramp up without incurring large human costs. This untapped productivity and “knowledge capacity” is being commoditized and accepted as a valuable resource.[95]

Businesses must be aware that if they outsource incorrectly, they risk losing control of the data and systems they outsource. Since AI’s commoditization of data is only in its early stages, these companies would have a competitive advantage. Waiting one, two, or three years to correct data control and commoditization could result in a major setback, given the widespread acceptance of data and AI. It may also be too late; businesses may never recover control of the same companies they once considered friends and allies.

It’s a basic concept: if you have one thing and someone gives you another, you now have two. If you send somebody water and salt, they will render salt water. When the salt is taken out, the person still knows how to make salt water even if the ingredients are no longer available. When using an AI method, if a neural network is given data and the computer absorbs information from its analysis, the machine still has the value of the acquired wisdom even if the data is deleted.

The ability to transfer data is evolving, and new outsourcing agreements can jeopardize a company’s ability to efficiently move and tailor its processes to how it needs things done or how its customers want things done.

1.5THE VALUE OF LEARNED INTELLIGENCE IN THE INSURANCE INDUSTRY

Let’s have a look at how a traditional insurance provider has dealt with upgrading and improving the claims process in recent years, especially the usage, value, and handling of data within that process. Although each business has its own procedure, this review is founded on a common methodology and understanding.[96]

Until about 60 years ago, insurance firms were responsible for contract issuing and placement, as well as managing all lawsuits. The administration of the claims process was then taken over by firms including Crawford and Co. and Gallagher Bassett. Third-party managers (TPAs) added structure and size to the claims

[95]SAFE HARBOR PRIVACY PRINCIPLES
http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/national%20laws/1USA_SAFE%20HARBOR%20PRIVACY%20PRINCIPLES.pdf

[96]Data Protection Technical Guidance Note: (PET) Privacy enhancing technologies (ICO)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf

resolution process. This was also combined with the use of outsourcing to countries like India, the Philippines, and other low-cost locations. After the 1980s, the principle of outsourcing has evolved significantly.

According to Fortunly, an organization "dedicated to demystifying financial processes, interpreting terms, and breaking down complicated transactions into basic measures," Nearly 54% of all businesses use third-party support teams to communicate with clients, and more than 93% of businesses have implemented or are exploring cloud platforms to increase outsourcing. Although data protection is a top priority for 68 percent of outsourcing firms exploring cloud adoption, more than "44 percent of chief intelligence officers report they are more likely to use outsourcing vendors than they were only five years ago."

In terms of claims management, outsourcing to a TPA or offshore still provided for a high level of process control. From the perspective of an insurance firm, it also owned and controlled the records, could customize the operation, and take advantage of size and cost savings. The insurer could travel to India or pay a visit to the TPA and direct its claims to the appropriate team. The data was also stored in files (databases) and maintained by departments inside the TPA or outsourcing company.[97]

Personnel and the main process is under the jurisdiction of the TPA, but the data could be picked up and transferred to another TPA, or even taken back in-house or outsourced again. Claims are routinely outsourced to lower-cost regions or businesses. The insurance carrier retains ownership of the data and the process at this stage, owing to the fact that it is manual or, at best, computer-based through some form of process automation. The insurance company's right to control or drive the process remains unaffected.

The TPA's key value proposition to insurers is expense, size, and management of the staff and team responsible for handling claims and adding value through their claim settlement expertise. The value of the TPA and the value of the insurance company are distinct.

With the integration of AI and machine learning into the claims process, a new breed of digital TPA, an AI enterprise, is emerging. On the surface, the value proposition seems to be the same as before, but with greater scaling potential and cost savings. The new business can provide opportunities to fundamentally alter how an insurer views risk. There is, though, a catch that you might not have seen before now. Although the TPA/AI firm might be providing a service, it is also acquiring an advantage that was previously unrealized and perhaps unaccounted for before the TPA/AI firm began its partnership with the insurance firm. When data is analyzed by an AI-powered TPA, insurance providers should be aware of the changing importance of data processing. The TPA may receive the value of the information gained from the data, and the insurer may lose a valued asset.

The TPA's AI technologies must be conditioned on the insurer's claim data in order to become professional at a particular mission. This may be the method of feeding data to the AI in the form of images, places, and words in order to train the neural network and create awareness. The insurance company's "data" feeds into the neural network. This training enables AI technology to function and succeed. The more data there is, the better the AI will be at performing the task. This technology is highly versatile and extremely useful. The value of learned knowledge could

[97] Under Pressure, India Mulls Steps to Protect Privacy (Vir Singh)
http://spectrum.ieee.org/telecom/security/under-pressure-indiamulls-steps-to-protect-privacy

eventually dwarf the value of individual details, similar to the adage, “Give a man a fish, and you feed him for a day; teach a man to fish, and you feed him for a lifetime.” The transition from using a TPA to populating a neural network with an AI-powered TPA is subtle but important. Building a project with a TPA to train an AI on the promise of faster claims settlement is good and efficient, as long as the insurance provider knows the benefit transfer as well. If this is what is explicitly understood in the contract, the value transfer should be quick and clear: the insurer gets an automatic process, and the AI business gets to develop AI applications that can scale on the insurer’s data. But, does the insurer realize that, while reaping the benefits of AI, it is still constructing a potentially strong brain for the outsourced service, making it possible for those to contend with it?

If the TPA uses a typical neural network, it is creating this “brain” using data from the insurance industry, and this acquired wisdom will never be returned to the insurance company without the TPA discarding its hard work and neural network. When a TPA handles claims for multiple insurers or self-insured entities, the experience and processes of one insurer/self-insured entity are leveraged for the good of the others. Although the images and other data that the TPA input and processed can be returned or discarded (as expected by certain service contracts), the data that filled and educated the neural network leaves acquired intelligence with the TPA that is difficult to erase.[98] If the learned intelligence is not returned or lost, the stored data may be resold to other insurers and self-insureds via the TPA’s services. As TPAs may boast that they provide more intelligence than every other insurer, the power shifts from a TPA simply providing an outsourced opportunity to a TPA providing an insurer with more knowledge and insights based on “industry” data derived from the original insurer’s processed data.

The presence of a common neural network also lowers the entry barrier for new insurers, who can simply hire an AI-powered TPA to handle claims without having to provide any initial details.[99] A new entrant no longer requires the expertise required to develop a massive claims enterprise in order to advise its underwriting and claims settlement. This ease of entry into the insurance industry can encourage well-capitalized financial and technology firms to enter the market as new insurance players, challenging long-established firms that have invested decades in their own processes.

1.6NEGOTIATE WITH UNDERSTANDING

Many insurers may decide not to invest capital or professional personnel in developing an automated AI claims process. As a result, they’ll have to outsource this task. Without the vast databases and learned expertise of insurers, an AI business would fail to have the claims automation that the insurer requires; as a result, the AI company and the insurer would need to collaborate.[100]The use of an AI-powered TPA arrangement by an insurer may be a perfectly suitable strategy. However, the parties to this transaction should be aware of whether the TPA is utilizing a common neural network, whether the learned intelligence can or should be

[98]Bob Whitehead, Invasion of privacy laws and video surveillance -- what’s legal, what’s not? http://www.video-surveillanceguide.com/3048-invasion-of-privacy-laws.htm

[99]Roger Clarke Visual Surveillance and Privacy http://www.rogerclarke.com/DV/VisSurv0508.html

[100]Tracy Mitrano, Civil Privacy and Legislative Security Policy http://net.educause.edu/ir/library/pdf/ERM0362.pdf

discarded, and whether it is entitled to the residual value of the learned intelligence acquired by the TPA as a result of the data processing. The transaction's parties must know the best questions to pose, have a shared sense of the importance of the learned information, and each party's understood objectives must be clear and contractual. The advantages of AI in the claims handling process and in underwriting may become ever more important in the years ahead, regardless of whether an insurer uses a common neural network or a segregated neural network. Rather than waiting for a contract to expire, the insurer and its AI-powered TPA should be constructive, recognizing and addressing these problems right away.

1.7 LET'S SUM UP

We have learnt about how artificial intelligence is used and how it can compromise your privacy if it's not handled properly. The TPAs need to be set up in such a way that the insurers will benefit from them.

1.8FURTHER READING

- Lin, J. C. W., &Yeh, K. H. (2021). Security and Privacy Techniques in IoT Environment.
- Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). Privacy Issues of AI. In An Introduction to Ethics in Robotics and AI (pp. 61-70). Springer, Cham.
- Michael J Quinn. Ethics for the information age (7th edition). Addison- Wesley Publishing Company, 2017. ISBN 978-0134296548 (Chap. 5).
- SareBaase and Timothy M. Henry. A Gift of Fire Social, Legal, and Ethical Issues for Computing Technology (5th Edition). Prentice Hall PTR, 2017. ISBN 9780134615271 (Chap. 2).

1.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What is a Third-Party Administrator (TPA)?**

   A third-party administrator is an organization that contracts with another company to offer operational services such as claims administration and employee health administration. Claims management is frequently outsourced by insurance providers and self-insured businesses.

1.10 ACTIVITY

Elucidate the relationship between AI and data privacy along with examples. (1000-1500 words)

Unit 2: DATA PROTECTION AND PRIVACY PROTECTION ON PUBLIC CLOUD

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Cloud Architecture and Security Issues

2.4 Cloud Data Security Challenges

2.5 Data Integrity Protection Methods

2.6 Data Privacy Protection Methods

2.7 Let's sum up

2.8 Further reading

2.9 Check your progress: Possible Answers

2.10 Activity

2.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- security issues relating to cloud architecture
- data integrity protection methods
- data privacy protection methods

2.2 INTRODUCTION

Because of its on-demand service and scalability capabilities, cloud computing has become a common technique. The cloud is most often used for data collection and big data or computation-intensive systems today. As a result, data protection and privacy has become a top priority, especially for business-related data. Data protection, transparency, and integrity are the three core aspects of data protection. The aim of data protection is to keep data collected in the cloud from being identified.[101] Data protection and privacy challenges remain in the cloud in the data life cycle, from generation to upload, usage, exchange, preservation, and archival.Data encryption and access management are often used with traditional data protection systems. And if the adversary obtains the data, data protection using AES or other encryption techniques will avoid valuable information from being leaked. However, due to high encryption and decryption overhead in storage and computing, it has reliability issues when working with oceans of data in a cloud world. The aim of access control is to deter unauthorized users from gaining access to records.[102]

However, in cloud computing, users may not have physical control of the machines on which they store data, and since the same physical machine can be used by multiple tenants thanks to virtualization, an adversary may monitor physical machine behavior to obtain valuable data from other tenants, and cloud providers are unreliable, they can accidentally or intentionally compromise data. Many studies have been conducted on the unique aspects of data protection in the cloud computing environment.

2.3CLOUD ARCHITECTURE AND SECURITY ISSUES

Both outsider and insider attacks pose a challenge in a public cloud world. Malicious code attacks, DDoS attacks, network eavesdropping, and so on are all examples of outsider attacks. The cloud infrastructure architecture has three levels. Each physical computer has several virtual machines (VMs) built in the infrastructure layer. Customers are provided with a portal by the platform layer. Customers can have their own software, programs, and configurations installed. The cloud vendors provide the software stacks across the software layer.A consumer on the client side may be a legitimate user or an actor impersonating legitimate users. Man-in-the-

[101]G. Ateniese, M. Steiner, and G. Tsudik ," Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. on Cloud Computing,2015.

[102]Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou , "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol . 25, issue. 1, 2014.

middle threats may also be carried out by network eavesdroppers.[103] To secure the whole cloud network, firewalls or intrusion detection systems (IDS) may be mounted. In the following chapters, we'll go through potential threats at various points and how to defend yourself.

a) Authentication:

End users and the cloud environment are all vulnerable to attacks during authentication. For authentication, most public cloud services today, such as AWS, use public/private keys. Users must first build and download a key pair created after logging in with their username and password. The key pair is used for further connection and authentication to EC2 instances.[104] However, in the middle of the network, eavesdroppers can intercept the main pair and do crypto analysis or a man in the middle attack. In this case, periodically updating the key pair and using multifactor authentication can be beneficial.

b) Virtual Machine Attacks:

Many tenants will use the same physical computer in the public cloud due to virtualization. If adversaries posing as legitimate users gain access to the virtual computers, they will be able to carry out attacks for the following reasons:

- Calls to a virtualized network interface are routed to a real network device. If malicious code is inserted, it can spread to other virtual machines on the same physical computer, and possibly to other physical machines.
- An adversary may execute attacks using relaxed access control and inter-VM contact on the same physical computer.[105]

c) DDoS attacks:

Since cloud services have a large number of servers, it will be difficult for attackers to launch DDoS attacks. However, once the opponent knows the location of the data, they will make the individual servers that host the user's data unavailable to access. Live virtual machine migration may be used to solve this problem. AWS, for example, offers a Virtual Private Cloud (VPC) solution for tighter access management.

d) Insider abuse:

Unlike single computers and pools, cloud computing machines are owned by cloud companies. Cloud vendors must have a good understanding of the data's contents, location, and computation/analytics approaches. Data stored in the cloud may be leaked if cloud vendors collude with adversaries. As a result, strategies for securing data in untrustworthy cloud services must be created. In the following pages, we'll go through some of the current processes, such as multiple storage.[106]

---

[103]Dev, H., Sen, T., Basak, M. , Ali, M.E. "An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks", High Performance Computing, Networking, Storage and Analysis , pp. 1106 – 1115, 2012.

[104]K. Hwang and D. Li, " Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, Vol.14, Sept. 2010.

[105]Yang Pan; GuiXiaolin; An Jian; Yao Jing; Lin Jiancai; Tian Feng , "A retrievable data perturbation method used in privacy-preserving in cloud computing", China Communications, vol. 11, issue 8, pp. 73-84, 2014

[106]Ming Li; Shucheng Yu; Kui Ren; Wenjing Lou; Hou, Y.T, "Toward privacy-assured and searchable cloud data storage services", IEEE Network, vol. 27, issue. 4, pp.56-62, 2013.

2.4CLOUD DATA SECURITY CHALLENGES

As previously said, there will be more data protection issues in a cloud setting than in a conventional single machine that is in the hands of the customers. Various issues and potential threats during cloud data use and storage processes are summarized in this section.

a) Data Use

As data is moved to the cloud, cloud administrators can have full access to everything customers have converted to cloud machine instances. The data collected in the cloud may be misused by both opponents and cloud vendors. As a result, data transformation will be required to avoid the loss of useful knowledge. Simple encryption is possible if the cloud is only used for data storage and no other operations are needed.[107]

However, in most cases, additional processing is needed. Users may need to do some processing on the data they've saved. Computations such as matrix multiplication, for example, may be required. For data classification, data mining approaches such as machine learning algorithms must be used.

The cloud is where data computation and analytics take place. However, some cloud data applications will necessitate coordination between local users and the remote cloud. Users can, for example, require the retrieval of specific data in order to modify it using data querying.

The below is a detailed description of the above cloud data use concern:

1) Encrypted data processing. The algorithms for data and computation-intensive software are often stored in the cloud. Cloud providers may deduce what types of data are processed based on the algorithms. Furthermore, in order to secure privacy, the data to be stored must be encrypted. The topic of how to process encrypted data without decryption remains unanswered.
2) An attack on query analytics. Significant amounts of data are stored in a cloud environment.[108] For auditing, sorting, or other processes, remote users must query data hosted in the cloud. For the following purposes, queries may be used to carry out attacks:
    a) These requests and queried answers will be obtained via an Internet link with eavesdroppers sitting in the centre.
    b) The cloud vendor is untrustworthy. Cloud providers have little visibility into the data handling procedures. Even if the original data is transformed

[107]Boyang Wang; Baochun Li; Hui Li, " Oruta: privacy-preserving public auditing for shared data in the cloud", IEEE Transactions on Cloud Computing, vol.2, issue. 1, pp. 43-56, 2014

[108]AlexandruButoi, NicolaeTomai, "Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach", 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing

and stored within, and the same query is translated to different values per time and sent to the cloud world, cloud providers will still be able to extract any information.

c) Prior knowledge of the data gathered from open databases may be paired with the empirical findings to derive useful details.

b) Data Storage

Users' data is maintained in remote virtual machine instances owned by service vendors in a cloud environment. External attacks on virtual machines may include malicious code attacks, breaching the associated Virtual Machine Monitor, and so on. Aside from the threat from the outside, consumers have no physical control over their files. Cloud providers' insiders could see just what was stored in their virtual machine instances. It would be a disaster if cloud providers' insiders collaborated with rivals to alter or leak customers' data on purpose.

Confidentiality, honesty, and availability are all aspects of data storage protection. How to avoid information theft and effectively verify data privacy over vast amounts of data stored in the cloud remains a concern in terms of data confidentiality. The aim here is to reduce the chances of recovering the original data from the hacked cloud storage system. In order to maintain data confidentiality, opponents and cloud vendors will purposefully alter the data. It is important to perform effective integrity checks on massive amounts of data. Customers' data will be inaccessible due to both system maintenance and threats in terms of data availability.

2.5DATA INTEGRITY PROTECTION METHODS

Data Modification Attack, Tagforgery and Data Leakage Attack, Replay and Timeliness Attack, Roll-Back Attack and Collusion Attack, and Byzantine Attack are all examples of data confidentiality attacks in the cloud. To maintain secrecy and integrity, a Trusted Cloud Computing Platform (TCCP) built on trusted computing is suggested. Each node has the trusted framework module installed. However, since users do not have power over the physical equipment, remote attestation is needed to ensure that the calculation comes from the virtual machine on which users are operating applications.[109]

A trusted platform module (TPM) is inserted in each virtual machine, and a trusted virtual machine monitor (TVVM) is enabled during booting. Furthermore, the attestation is performed by an external trustworthy coordinator (TC). Digital nodes must first register with TC. TPM-based Intel Trusted Execution Technology (TXT) is already available. It's compliant with OpenStack, an open-source cloud computing software framework. It contains an Open Attestation registry that communicates with the trusted computing pool of hardware and software. With trusted cloud storage,

[109]Y. Kajiura, A. Kanai, S. Tanimoto, and H. Sato, "A file distribution approach to achieve high availability and confidentiality for data storage on multi-cloud," in Computer Software and Applications Conference Workshops (COMPSACW) 2013 IEEE 37th Annual. IEEE, 2013, pp. 212–217.

however, program level attacks will be undetectable. For instance, if data in a database is corrupted. That would be undetectable. Additional application-level authentication must be enforced in order to use TCCP.

2.6DATA PRIVACY PROTECTION METHODS

Anoymization is a technique that can be used. By hashing the unique identifiers of each row, a unique indexing[110] of each row in the database is created. The hashing information must be maintained locally, and the table must be separated by columns to separate cloud providers after these specific identifiers are removed. Person anonymity is preserved in this manner; but, since the whole column would be stored in a single cloud, data mining attacks may be used to anticipate valuable information.

2.7 LET'S SUM UP

This chapter reflects on the confidentiality and privacy of data collection and computation. Different approaches are compared, and issues and benefits of current methods are discussed. To deal with anonymization, authentication, data processing with separate operations, and secret stage, a hierarchical multi-cloud architecture with a shared pre-processing API and local database is proposed. By calling a generic API, the proposed architecture may include different authentication methods based on the data type and use, reducing complexity. However, there are a few issues with this design that need to be addressed: a) The call to the standard API will be resource intensive, necessitating caching and flexible procedures. b) Although the majority of computing and computation is performed in the cloud, some pre-processing and data-related information must be processed and managed locally. c) Since algorithms are used on encrypted data, customer-oriented algorithms must be created. Users must provide a thorough understanding of cryptographic files and a fully integrated framework benchmark must be developed, applied, and analyzed using quantitative and qualitative performance measures.

2.8FURTHER READING

- G. Ateniese, M. Steiner, and G. Tsudik ," Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. on Cloud Computing, 2015.
- Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou , "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol . 25, issue. 1, 2014.

[110]A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp.612-613.

- D. Chen, and Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” IEEE International Conf. Computer Science and Electronics Engineering (ICCSEE), pp. 647-651, March. 2012.
- Dev, H., Sen, T., Basak, M. , Ali, M.E. “An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks”, High Performance Computing, Networking, Storage and Analysis , pp. 1106 – 1115, 2012.
- X. Huang, X. Du, “Efficiently secure data privacy on hybrid cloud”, IEEE International Conference on Communications, pp. 1936-1940, 2013.

2.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the three layers of cloud computing platform?**

The cloud infrastructure architecture has three levels. Each physical computer has several virtual machines (VMs) built in the infrastructure layer. Customers are provided with a portal by the platform layer. Customers can have their own software, programs, and configurations installed. The cloud vendors provide the software stacks across the software layer.

2.10 ACTIVITY

Based on the role of data privacy and its integrity, explain how the breach if privacy can be protected and why is it necessary based on your opinion. (900-1000 words)

Unit 3: PRIVACY ISSUES AND DATA PROTECTION IN BIG DATA

3

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Privacy Issues in big Data Analytics

3.4 Let's sum up

3.5 Further reading

3.6 Check your progress: Possible Answers

3.7 Activity

3.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Impact of data security legislation on big data programs
- Privacy issues in big data analytics
- General Data Protection Regulation

3.2 INTRODUCTION

Big data refers to vast or diverse quantities of organized or unstructured data that can be used to provide value. Big data is typically described by a number of V-properties, such as length, velocity, and variety. Big data has now become a form of finance, with businesses vastly improving their processes and customer relations, and academics creating and enhancing science. Furthermore, the massive volume, rapid generation, and diversity of data necessitate unique storage and processing architectures.[111]

Although big data analytics has a lot of benefits, it also has a lot of privacy concerns when dealing with sensitive information. This is attributable to two elements of big data processing in particular. First, the more data there is, the more likely it is to re-identify people, often in databases that seem to lack personal linking knowledge. Second, big data research will infer new information from "harmless" personal data that is much more sensitive and was not meant to be disclosed by the individual affected.[112] A well-known example is a department store's study of purchasing habits in order to create personalized (targeted) ads, in which the algorithms accurately concluded that a young girl was pregnant. In other cases, such as medical care or testing, privacy risks can become much more severe.[113] A variety of technological means and legislation for privacy-preserving data collection have been introduced and developed in order to safeguard persons and their data.However, incorporating these techniques into a data processing system necessitates extra work during the design phase, and in many cases, such methods have an impact on the system's performance. As a result, companies and other organisations have not always been able to make this effort in the past, but this is changing as a result of recent privacy legislation and regulations.[114]

This unit discusses privacy challenges in big data processing and delves into two case studies that see how legitimate privacy standards can be fulfilled in big data and extremely sensitive personal data research ventures. Finally, it addresses the effects of the privacy-preserving approaches used on data collection and the outcomes.

---

[111] *NIST Big Data Public Working Group Definitions and Taxonomies Subgroup, "NIST Big Data Interoperability Framework: Volume 1, Definitions," National Institute of Standards and Technology, Tech. Rep. NIST SP 1500-1r1, Jun. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf*

[112] *Gartner IT Glossary, "What Is Big Data?" 2018. [Online]. Available: https://www.gartner.com/it-glossary/big-data*

[113] *K. Hill, "How Target figured out a teen girl was pregnant before her father did," Forbes, Inc, 2012.*

[114] *J. T. Overpeck, G. A. Meehl, S. Bony, and D. R. Easterling, "Climate Data Challenges in the 21st Century," Science, vol. 331, no. 6018, pp. 700–702, Feb. 2011.*

3.3PRIVACY ISSUES IN BIG DATA ANALYTICS

A. Legal Regulations

From a legal standpoint, the EU General Data Protection Regulation (GDPR), which took effect in May 2018, is the subject of this article. If an organisation processes data of European residents, it is applicable to all organisations within the European Union (EU), the European Economic Area (EEA), as well as organizations from other countries. As a result, the GDPR affects the majority of large corporations around the globe.[115]

The GDPR governs how personal data is collected, stored, and processed. Any data that can be attributed to a single individual being is considered personal data. Which contains not just overt personal identification (such as full name and national ID number), but often indirect identifiers such as phone numbers, IP addresses, and photographs of recognizable individuals. Data without such identifiers is generally known as anonymous and falls outside the GDPR's domain (Recital 26).Big data analysis also yields observational conclusions with no causal connections to real people. As a result, processing only anonymous data is an easy way to comply with all GDPR specifications. The concept of anonymity, on the other hand, is not straightforward.[116]

Even if directly identifiable parameters are omitted from a dataset, combining the dataset with other information can allow single individuals to be re-identified. Background information assault is the term for this method of de-anonymization. The Netflix challenge in 2006 is a well-known case of re-identification. Netflix launched a dataset featuring 500,000 consumer movie reviews as part of a competition to discover more reliable movie recommendation approaches. Any personally identifiable information (PII) was excluded from the dataset, leaving only subscriber IDs (with no connection to the actual identity) and movie ratings (score, movie info, and date). However, researchers were able to classify particular consumers with a high likelihood by combining these data with other publicly available information (e.g., IMDB ratings).[117] Such well-known examples include identifying people based on their search words on the internet, anonymized DNA, and mobility info.

There are a variety of systematic metrics for determining a dataset's degree of anonymity (see next section). Since the GDPR does not have a clear or concrete concept of anonymity, it finds a dataset anonymous where re-identification is only possible through a great deal of difficulty or by impossible means. The GDPR establishes a set of legislative, bureaucratic, and technological standards for the collection of personal data, as well as various approaches. The most important concepts are outlined in this section. To begin with, in most instances, personal data collection is only permitted if the data subject has given his or her permission (Article 6).Exceptions occur when data collection is expressly permitted by statute or policy,

---

[115] *V. Marx, "Biology: The big challenges of big data," Jun. 2013. [Online]. Available: https://www.nature.com/articles/498255a*

[116] *M. Mostert, A. Bredenoord, M. Biesaart, and J. J. Delden, "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach," European Journal of Human Genetics, vol. 24, no. 7, pp. 956–960, Jul. 2016. [Online]. Available: https://www.nature.com/articles/ejhg2015239*

[117] *A. Machanavajjhala, M. Venkitasubramaniam, D. Kifer, and J. Gehrke, "L-Diversity: Privacy Beyond k-Anonymity," in 22nd International Conference on Data Engineering (ICDE'06)(ICDE), 2006, p. 24. [Online]. Available: doi.ieeecomputersociety.org/10.1109/ICDE.2006.1*

or when it protects the data subject's "vital interests." Furthermore, approval must be limited to a single reason for data collection (Article 5). The data controller (the person in charge of gathering the data) cannot identify a too broad data collection function or alter it later on at will. Another data management theory is data minimization (Article 5), which refers to restricting personal data collection, storage, and use to data that are valid, sufficient, and, most significantly, essential for the processing intent. It's worth noting that pseudonymization is listed as a data minimization technique.[118] Identifiable parameters are replaced by other (randomly) generated identifiers in pseudonymized data. This typically has little detrimental effect on the data mining process and can be done by the data controller prior to moving the data to the data processor.

The data controller, which contains the mapping (also known as a pseudo-lookup table) pseudonyms to the recognizable parameters, can be used to relate the data processing performance. Aside from anonymized data, storage at the data controller must comply with the GDPR by using strategies that encrypt data in transit. Furthermore, Article 32 of the GDPR mandates the use of "effective technological and operational steps to ensure a degree of security appropriate to the danger," which generally entails the use of data encryption, access management, physical security, and (once again) pseudonymization.[119]

The storage restriction theory is an extension of the data minimization principle, which limits the length of data storage to a given (necessary) time. In the sense of data collection, it is also worth noting that automated decision-making procedures that have an effect on persons (Article 22), as well as the processing of highly sensitive data, such as biometric data (Article 9), need the data subject's "explicit" permission.

The GDPR does not explicitly answer the words "big data" or "data mining." Big data and the GDPR, on the other hand, are not always compatible, as the above definition shows. Big data mining, for example, focuses on the processing of vast volumes of data, which also goes against the data minimization concept. Furthermore, once the data has been compiled, new ideas for research are often introduced in data processing. The data subjects from whom the data were gathered, on the other hand, had originally given their permission for a different reason. As a result, from a legal standpoint, data collection should be performed on anonymized data wherever possible; otherwise, careful caution must be taken to ensure that the GDPR is followed. This could necessitate a data protection impact assessment (DPIA), which is a privacy-related impact assessment whose aim is to identify and analyze how certain acts or practices may affect data privacy (Article 35).

B. Technical Aspects

Technical means must be used to implement the legal specifications presented in the previous section. This segment discusses several privacy-preserving data mining techniques. The works of Agrawal and Skrikant, as well as Lindell and Pinkas, are well-known early approaches in this field.

---

[118] *D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, ser. SIGMOD '11. New York, NY, USA: ACM, 2011, pp. 193–204. [Online]. Available: http://doi.acm.org/10.1145/1989323.1989345*

[119] *A. Narayanan and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," in 2008 IEEE Symposium on Security and Privacy (sp 2008), May 2008, pp. 111–125.*

In the first, data was distorted to make it anonymous, and then the anonymized data was subjected to a special decision tree classification analysis. In the second, the data was divided into two different datasets (a process known as pseudonymization), and a special multi-party computing algorithm was created to analyze the dataset.[120] This diagram depicts the common components of privacy-preserving data analysis: anonymization (as powerful as possible; at the very least pseudonymization) and possibly mining algorithms tailored to this type of updated data.
The attributes in a dataset are normally divided into four groups to aid in the anonymization process:

- Explicit identifiers: features that can be linked to a certain person, such as a social security number or an email address.
- Quasi-identifiers: attributes that do not explicitly connect an entity, but when the meanings of several attributes are merged, they will re-identify the person. Date of birth, ZIP code, and occupation are some examples.
- Sensitive data: features representing material that the data subject does not want exposed or, at the very least, not related to its identity. Diseases, financial situations, sexual identity, and current employment are some examples.
- Non-sensitive data: characteristics that do not fit into any of the previous categories (e.g., weather data).[121]

Unfortunately, this classification is not always clear: a (rare) disorder may also be used to classify a human. There are significant variations between the groups as well: the place of residence as a quasi-identifier may apply to millions of citizens in a big city, but just a few persons in small villages. A variety of anonymity models exist to measure the rate of anonymity and hence the threat of re-identification.
It is true that confidential knowledge is always of great importance to data miners, but also to adversaries. If the purpose of an analysis is to attach explicit identifiers to sensitive data, anonymization is clearly impossible, and the GDPR must be considered. In the very least, pseudonymization should be included in this situation. Data mining, on the other hand, is often used to find relations between quasi-identifiers and critical attributes, allowing data to be anonymized. Common anonymization methods are:

- Suppression: eliminating the values of an attribute entirely or replacing them with a dummy value (typically an asterisk "*") is a popular anonymization process. Explicit identifiers are commonly used for this operation.
- Generalization: within the attribute taxonomy, replacing attributes with more generic or abstract values, such as date of birth age (in years); age (in years)

[120] *J. Bohannon, "Genealogy Databases Enable Naming of Anonymous DNA Donors," Science, vol. 339, no. 6117, pp. 262–262, Jan. 2013.*
[121] *T. Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall L. Rev., vol. 47, p. 995, 2016.*

a number of years; ZIP code first two digits Normally, this operation is performed on quasi-identifiers.

- Permutation: grouping the data and shuffle- fling the sensitive values within each section. As a result, the link between quasi-identifiers and sensitive data is broken.
- Perturbation: replacing values in such a way that the original data is no longer connected, but the mathematical properties remain the same. Adding noise is a popular technique for perturbation.[122]

The presented models and anonymization methods are not only academically interesting, but they are also used in realistic privacy guidance (e.g., the Norwegian data protection authority). The foregoing anonymization operations undoubtedly result in the lack of metadata and a reduction in the data's utility. One may compare various anonymization methods to find the trade-off between privacy and utility using the utility and confidentiality metrics.
Mining anonymized databases often necessitates the use of specifically tailored mining algorithms. Decision trees, Bayesian classification, support vector machines (SVM), and stable multi-party computation are examples of classification and clustering algorithms that have privacy-preserving variants.

3.4 LET'S SUM UP

This chapter discussed the impact of data security legislation on big data programs and examined how privacy-preserving approaches can be implemented using two case studies. The outcomes were strikingly different. Participants in one study were asked to contribute to the collection and processing of biometric data in order to alleviate privacy issues. Furthermore, there were no issues during the data processing process. Data from an internal data base was included in the second project. Many data fields had to be anonymized, which made data processing more difficult and, in many cases, restricted. It is important to note that for programs and applications that deal with sensitive data, a data security impact review should be carried out at the very beginning of the project to recognise possible privacy issues and to adapt the research methodology to take privacy-preserving strategies into account.

3.5FURTHER READING

- J. T. Overpeck, G. A. Meehl, S. Bony, and D. R. Easterling, "Climate Data Challenges in the 21st Century," Science, vol. 331, no. 6018, pp. 700–702, Feb. 2011.

[122] *R. Agrawal and R. Srikant, "Privacy-preserving Data Mining," in Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, ser. SIGMOD '00. New York, NY, USA: ACM, 2000, pp. 439–450. [Online]. Available: http://doi.acm.org/10.1145/342009.335438*

- T. Z. Zarsky, “Incompatible: The GDPR in the Age of Big Data,” Seton Hall L. Rev., vol. 47, p. 995, 2016.
- A. Narayanan and V. Shmatikov, “Robust De-anonymization of Large Sparse Datasets,” in 2008 IEEE Symposium on Security and Privacy (sp 2008), May 2008, pp. 111–125.

3.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. What is covered under GDPR?

The GDPR governs how personal data is collected, stored, and processed. Any data that can be attributed to a single individual being is considered personal data. Which contains not just overt personal identification (such as full name and national ID number), but often indirect identifiers such as phone numbers, IP addresses, and photographs of recognizable individuals.

3.7 ACTIVITY

Analyse through case studies the privacy issues and the application of GDPR. (900-1000 words)

Unit 4: PRIVACY AND DATA PROTECTION LAWS IN INDIA

4

Unit Structure

4.1 Learning Objectives

4.2 Introduction

4.3 Constitutional Status

4.4 Analysis of the Right Based Approach

4.5 Data Protection & Information Technology (Amendment) Act 2008

4.6 Data Protection & Corporate Affairs

4.7 Let's sum up

4.8 Further reading

4.9 Check your progress: Possible Answers

4.10 Activity

4.1 LEARNING OBJECTIVE

After going through this chapter, you should be able to understand:

- Data protection under the Indian Constitution
- Data Protection and Information Technology Act
- Data protection and corporate affairs

4.2 INTRODUCTION

In the international and national spheres, rights, which are intrinsic and inalienable characteristics of human society, have been reduced to a tangible and implementable text. Certain rights are stated explicitly in such texts, while others are introduced by an interpretative tool due to their integral relationship with other rights. One of the most significant and legitimate personal rights is the right to privacy. Person snooping from others gains influence as a result of it. The Universal Declaration on Human Rights, International Covenants on Civil and Political Rights, and the Convention on the Rights of the Child all mention the right to privacy.[123]

The right to privacy is one of the most important aspects of human life. This right has been described in India as an intrinsic part of the right to life and liberty, as well as the right to freedom of expression. A citizen is entitled to a "personal domain" that is free of unjustified state or third-party control or surveillance. Despite widespread awareness of the duty to respect privacy, universal human rights security systems are yet to adequately develop the precise content of this right. The lack of a consistent statement of the substance of this right has made its implementation and compliance more complex.

Since the right to privacy is a qualifying right, interpreting it poses difficulties in determining how the private domain is organized and defining conceptions of what constitutes public interest. The right of a human being has been encroached upon as a matter of general concern by the means of communication. Individuals should share knowledge and ideas in a room that is beyond the control of other members of society, the private sector, and potentially the State itself, according to the study of privacy of communications. Individuals should only use these protections to exercise their right to privacy in a communications scheme. The documentation of a right relating to non-interference with one's personal life occurred in the mid-nineteenth century. Through the commodification of technology, it has gained meaning. Any aspect of human life has been impacted by technology. The intrusion of modern technologies into human culture has been a daily occurrence.[124] It occurs either as a result of voluntary disclosure or as a result of unintentional knowledge collection. Demands for strict guidelines regulating the gathering and storage of personal information arose as a result of the monitoring capacity of powerful computer systems. The origins of contemporary laws in this field can be traced back to the first data security statute in the world, which was based on individual privacy. Data security is a form of privacy that has become a global phenomenon in recent years.

[123]Ghosh, Dr.Jayanta& Shankar, Uday. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.

[124]Prakash Shah, "International human Rights: A perspective from India," Fordham International Law Journal, Vol. 21, Issue 1, Article 3, (1997): 24- 38.

The concept of defining data privacy as a civil right is a novel one. If a person has the right to privacy, he or she also has the right to data protection. Even with the current technical advancements, data security is also an emerging area.[125]

4.3CONSTITUTIONAL STATUS

There are some clauses in India's constitution which include "Freedom of Speech and Expression" and "Right to Life and Personal Liberty." The right to privacy as a human right is affected by these provisions. There have since been a variety of occasions where the right to privacy has been established as a constitutional right. This proposition's conceptuality is often linked to the current dimension of "Data Protection." The relationship between privacy and data security is inextricably linked. The right to data privacy is inextricably linked to an individual's "data."The analysis of constitutional provisions in order to comprehend the relationship between privacy and specifically scripted rights, as well as the explanation given by the country's highest court.[126] It looks at how various laws cope with the problem of data security. Finally, it makes a case for approaching data privacy issues from a rights-based perspective. "Human rights are rights enjoyed by all human beings at all times and in all places, purely by virtue of their humanity," Sir John Simmons says of human rights. Universality, freedom from social or legal recognition, naturalness, inalienability from social or legal recognition, naturalness, inalienability, non-forfeit ability, and imprescriptibility may be among their properties. An account of human rights can only be interpreted in this manner if it captures the central concept of rights that can be asserted by any human being at any time."

As a result, the principle of protecting civil rights also includes data security. For a person, the universality and freedom of data security are critical considerations. The right to privacy is therefore protected as a result of data security.[127] The most important and illuminating point is that privacy and data security are not mutually exclusive. These connections or shadows represent various fields that are interconnected with this regime. Privacy, like seclusion, solitude, and loneliness, is a concept similar to seclusion, solitude, and isolation, though it is not associated with these terms; it goes far beyond the strictly abstract facets of privacy, such as detachment from the business, fascination, and others' power, meaning the right to exclusive control of access to individual realms. The court's advocacy as a pathfinder of this developmental right is now being emphasized as a matter of right. Human rights should be acquired naturally, so the right of privacy must be acquired naturally as well.[128]

4.4ANALYSIS OF THE RIGHT BASED APPROACH

Only by various legislations will the right-based solution to the "data privacy" problem be scrutinized. The aim of this approach is to examine India's "data security" regime

[125]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (1890): 193-220.

[126]Article 21 & 19 (1)(a) of the Indian Constitution, See also Udai Raj Rai, Fundamental Rights and their enforcement, PHI Learning Private Limited, New Delhi, (2011) p.19. See also Kharak Singh v. The State of U.P. and Ors. AIR 1963 SC 1295

[127]S.K. Sharma, Privacy Law: A Comparative Study (Atlantic Publishers & Distributors: 1994).

[128]Austin, Lisa Michelle, "Privacy law and the question of technology." Ph.D. Thesis, University of Toronto; 2005, ProQuest Dissertations and Theses.

from a global perspective. The topic of data security has gained a lot of traction in recent years, thanks to the growth of internet-enabled services, and has resulted in a surge in data collection, business process outsourcing, call-center services, accounting functions, and other corporate activities being outsourced.[129]However, as technology advances, so does the need to address the progress of legislation. As a result, data security enquires into the extent to which individuals' and organizations' identities, details, and data are covered under Indian law, particularly the Indian Constitution.

The defense provided by the Indian Constitution is highlighted because it is the "basic and ultimate root" from which all other laws derive their authority and power. (1) Privacy rights of interested parties in physical and cyber space, which these three shall present for discussion of constitutional aspects concern. (2) Freedom of communication obligations under Article 19 (1) (a). (3) Article 21 mandates the right to information of the general public. It categorically discusses the right to privacy, the right to access, the right to know, and electronic government, as well as trade secrets, intellectual property, and other topics from various perspectives. This analysis was carried out in order to clarify the association of rights. Furthermore, there is no equilibrium between knowledge and data processes, which is another flaw in this job.

The terms "data security" and "right to privacy" are being increasingly interchangeable. The 'personal security' will only be achieved if the invasion of privacy is halted. In general, and informational privacy in particular, privacy regulation has always been inextricably tied to technical advancement. Warren and Brandeis lament the "instantaneous images and newspaper enterprise that have violated the sacred precincts of private and domestic life; and countless mechanical machines threaten to make good the prediction that "what is whispered in the wardrobe shall be declared from the house-tops" in their seminal 1890 essay "The Right to Privacy." This is where the issue of privacy began.[130]

This is now being developed in the field of 'data security.' The concept of 'Data Protection' has many facets. The many facets of data security as a right, such as the right to access to data banks, the right to verify their accuracy, the right to update and amend them, the right to the secrecy of personal data, and the right to allow their dissemination: both of these protections are now combined to form the modern right to privacy. As a result, as a right-based policy, the linkage between "Data Protection" and "Privacy" status is quite reasonable in this case.

The appellant in R Rajagopal v. State of Tamil Nadu was the editor, printer, and publisher of a Tamil weekly magazine published in Madras who requested an injunction prohibiting the State of Tamil Nadu from intervening with the legal publication of Auto Shankar's autobiography, which was based on public records. In this case, Jeevan Reddy, J reaffirmed that the right to privacy is implied in Article 21 of the Constitution's protection of life and liberty. The Court has reiterated that every resident of this country has the right to be left alone in order to protect their privacy. As a result, the issue of "personal security" is developed in its own way by the "right

[129]Lee A. Bygrave, "Privacy and Data Protection in an International Perspective," Stockholm Institute for Scandinavian Law, (2010).

[130]Nicholas D. Wells, PoorviChothani and James M. Thurman, Information Services, "Technology, and Data Protection," The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009 (2010): 355-366

to privacy." In the same way, both ideas have been classified as a matter of right under the Indian Constitution.

4.5DATA PROTECTION & INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The terms "data privacy" and "Information Technology Act" have different implications in comparison to each other. The Act's goals expressly state that the security of cyber-relationships is a priority.[131] It ensures the data from information networks is protected from any types of breaches. The said Act contains protections aimed at preventing the unauthorized usage of servers, information networks, and data stored on them. Several clauses relating to "data security" have been added to the bill. The updated sections 43A and 72A of the Act talk specifically to data security. This 2008 Amendment Act is a major move forward in the fight against the plethora of cybercrime. The reforms in Indian legislation on constitutional data security have finally yielded to the demands of the United States and European nations over the last decade. The service provider is now serving jail time for violating a contractual requirement by disclosing "sensitive knowledge." Furthermore, revealing "private personal details" leaves the victim responsible for damages.[132]
As a result, privacy security has been granted the same position as a matter of right. The key emphasis given to analyze the EU Data Protection legislation and the stands of the Indian Information Technology Amendment Act 2008 is technical growth. In terms of the Information Technology Act 2008, it discusses the corporate use of data such as waste, share, discloser, publication protection measures, and penalties. Another example is the IT Rules 2011, which gives the appearance of presumption of right interest in its clauses. The significance of India's outsourcing industry and how it can affect the flow of business from European Union firms. This essay also discusses the newly notified legislation pertaining to the security of confidential personal data, as well as the Indian regulations, comparing their requirements with the UK Data Protection Act 1998 at times. As a result, the primary right-based approach to human privacy security is claimed.

4.6DATA PROTECTION & CORPORATE AFFAIRS

The alliance between "data privacy" and "corporate affairs" is now forming a right-base strategy. The business world is seriously impacted in a variety of ways. The importance of data entry, disclosure, sharing, and processing cannot be overstated. In the business world, data processor or data manager custody has played a critical part.[133] It is sometimes the duty of a private company to share or not to share information. This is where private and charitable organizations clash with law enforcement agencies. When someone tries to view details or place an order for a product, the ad online will prompt them to fill out a form.

[131]Bygrave, L.A., "Data Protection Law: Approaching Its Rationale, Logic and Limits," Kluwer Law International, The Hague / London / New York (2002).
[132]Justice A P Shah Committee Report, "Report of the Group of Experts on Privacy", (2012), Accessed October 21, 2016, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.
[133]H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191,

Now the question is whether the data retained by the authority after application of this information complies with public policy. In terms of this, in the banking industry, the banker has a responsibility not to reveal information in their hands, resulting in a violation of the client's duty of privacy and confidentiality. The extent of a banking customer's right to privacy was limited because it interfered with the right to access and public information. The Securities and Exchange Board of India Act (1992) established the Securities and Exchange Board of India (SEBI) to control and regulate the use of people's credit records. The government's reactive control is mediated by the Security Exchange Board of India, which is given limited access to private-sector data relating to the stock market under the Act. As a safeguard against unauthorized reactive access, SEBI is only allowed to inspect if it has reasonable grounds to believe that: a company has engaged in insider trading or fraudulent, unfair trading practices have been used, securities transactions have been handled in a way that is detrimental to the investor,[134] or an intermediary or any person associated with the securities mafia has been involved in insider trading or fraudulent, unfair trading practices have been used, or an intermediary or any person associated with the securities market is contravening any provision in the Act.

By penalizing someone who fails to have the necessary information, the Act reinforces reactive access to and dissemination of information. The Credit Information Companies Regulation Act, 2005 ("CICRA") mandates that credit information belonging to persons in India be obtained in accordance with the CICRA regulation's privacy standards. Entities responsible for processing and storing the data have been held accountable for any potential data exposure or modification. The CICRA also established a stringent system for details relating to credit and finances of individuals and businesses based on the Fair Credit Reporting Act and the Graham Leach Bliley Act.[135]

The Reserve Bank of India recently informed the CICRA Regulations, which establish strict data privacy principles. As a result, the fields of "data security" and "corporate relations" are moving in the same direction as the "right-based solution."

4.7 LET'S SUM UP

Data security has been viewed as a right from various perspectives, according to the study of various themes. All of the subjects, such as the right to privacy, the right to records, information security, and corporate relations, were emphasizing the importance of accepting data security as a right. In this age of technical liberalization, the aim of the issue is to reinforce the view of data privacy as a right. The reach of technology is expanding all the time, and in order to keep up with this trend, the data privacy regime must be strengthened in order to safeguard individual liberty. The aim of this chapter is to define the right to privacy and data security as a constitutional right that is warranted to regard as such after study. Only the entire legal provision as a right to data privacy will satisfy others' intrusion and infringement of individual liberties. Data security can take on a universal approach depending on the institutional standing. To grant data protection a special status as a right, the various

[134]Dr. Amit Ludri, Law on protection of personal & official information in India, The Bright Law house, New Delhi, 1st Edition, (2010).

[135]Praveen Dalal, "Data Protection laws in India: A Constitutional Perspective," Accessed October 21, 2016, http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-ININDIA.pdf.

aspects of data protection, such as data collection, transmission, storage, confidentiality, and access, should be brought together in a legal context. Knowledge of the proper foundation approach to data security and privacy must be universally distributed.

4.8FURTHER READING

- Dan Jerker B. Svantesson, “Systematic Government Access to Private Sector Data in Australia,” 2/4 International Data Privacy Law, (2012).
- Denis O’Brien, “The Right of Privacy,” Columbia Law Review, Vol. 2, No. 7 (1902): 437-448.
- Daniel J. Solove & Paul M. Schwartz, “Privacy, Information and Technology,” Wolter Kluwer Law & Business Publisher in New York, (2011), 79-256.
- M. M S Karki, “Personal Data Privacy & Intellectual Property,” Journal of Intellectual Property Rights, Vol 10. (2005): 59-63

4.9CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are special and general rights?**

   Special rights are derived from ‘special transactions [or] particular relationships,’ such as commitments, contracts, or political association membership, while general rights are derived from ‘all men capable of choice...in the absence of those special circumstances which give rise to special rights.’

4.10 ACTIVITY

Based on the data protection laws discussed in the chapter, critically analyse the implementation of such laws and recommend solutions to the same, if any. (900-1000 words)

Block-4

INTERNATIONAL LAW ON DIGITAL RIGHTS

Unit 1: INTERNATIONAL LAW ON CYBER SECURITY IN THE AGE OF DIGITAL SOVEREIGNTY

1

Unit Structure

1.1 Learning Objectives

1.2 Introduction

1.3 Existing challenges on international law and governance on cyberspace.

1.4 Digital Sovereignty in India

1.5 International law on cyber space and digital sovereignty

1.6 Concluding remark

1.7 Let's sum up

1.8 Further reading

1.9 Check your progress: Possible Answers

1.10 Activity

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- human rights perspective of cyber governance
- fundamental freedoms in digital space

1.2 INTRODUCTION

Through the use of cyber technologies such as the Internet and mobile devices, good cyber governance must create a human rights-based strategy for (1) more openness, (2) more openness, and (3) more stakeholder involvement. Furthermore, good cyber governance promotes and protects human rights through technology. Cyberspace, though, is a borderless public space in which people, regardless of their citizenship, race, sex, political affiliation, or gender collaborate and connect.[136] Cyberspace and the Internet are used by individuals to perform business, make policy, and organize their personal lives. Yet this space does not have any common rules or standards, a governance apparatus, or enforcement or control mechanisms that would protect and foster people's activities. Universal human rights principles and guidelines will act as guides and benchmarks for setting up governance systems in cyberspace. Cyberspace, thanks to emerging technology, provides an arena with a large number of people that can impact and manipulate one another. This room is clear and impartial by default, but the people who use it often identify, enlarge, restrict, or censor it. Internet correspondence is mostly private and used and exchanged with the public worldwide, who normally stays unknown to the actual Internet user; specifically, each of us. We nonetheless share our most sensitive and confidential data with this anonymous group.This modern, open society now has between 2 and 7 billion Internet users. If cyberspace were a nation, it would be the largest and most populous in the world, although one without any constitutions or government. There are no legislative or other political decision-making bodies in this "room."[137] It has no police or law enforcement system, let alone security mechanism to uphold human rights for all Internet users. Therefore it can be argued that (i) cyber governance does not need new human rights norms or standards, but rather new governing and monitoring regimes and enforcement mechanisms that guarantee and safeguard the human rights of all people who use cyberspace; (2) we need to identify all private, public, governmental, and international actorswho carry responsibilities in either violating or fostering human rights in the Internet; and (3) all users need to establish mechanisms that enhance trust in institutions (e.g., governments), companies (e.g., Internet providers, servers), and organizations (e.g., Facebook, YouTube).[138]

1.3CYBER GOVERNANCE AND HUMAN RIGHTS

[136]Eugen, Petac&Petruţ, Duma. (2019). Exploring the New Era of Cybersecurity Governance. AnaleleUniversitatiiOvidius Constanta. XVIII. 358-363.

[137]Aitel, D. (2013). Cybersecurity essentials for electric operators. The Electricity Journal, 26(1), 52-58.

[138]Allen, J. Governing for Enterprise Security. Pittsburgh: Carnegie Mellon University, 2005. Available on:

On one hand, the Internet and cyberspace can foster and enhance individuals' inclusive participation and access to politics and business, which they otherwise would not have. On the other hand, it can also exclude those who are Internet-illiterate or have difficulty accessing the Internet (e.g., children, aging people, and people without Internet-access). Billions of Internet users have now developed anonymous twin-identities in this new space by exchanging private information in cyberspace, without ever getting the opportunity to erase the information. Personal relationships and friendships established via social media platforms such as Renren and Facebook will seem to be private while revealing a wealth of personal information; as a result, it is a space for public privacy.[139]Anyone with access to this infinite room can now deal with businesses and companies, schooling and training, investments and economics, private communications, and even health and personal matters. Finally, a strong cyber governance system is absent in cyberspace: a quasi-government or governance regime that oversees the interests and claims of its people through oversight and compliance bodies.Although international governmental organizations (IGOs) such as the United Nations (UN), the Organization of American States (OAS), the African Union (AU), and the European Union (EU) aim to establish international standards and legally-binding treaties for the use of cyberspace and the Internet, they frequently fail to do so. Since their mandate to uphold human rights is entirely dependent on state authority and governments, each state's powers and compliance capacity always stop at state boundaries.

Also, IGOs and international courts often have limited measures and means to protect human rights, let alone enforce them.Since cyberspace has no physical or national boundaries, the methods for governing this current borderless regime are still being developed. Human rights norms and principles, such as the right to privacy, protection, health, free speech, movement, and industry, offer guidelines to the various players engaged in the regulatory design of the cyberspace regime in the debate and attempt to set up a cyberspace governance regime. If established, the cyberspace governing body will consist of multiple stakeholders and actors. This includes national,international, as well as private actors such as representatives of companies, social networks, NGOs, and individuals. The World Internet Governance Forum under the UN has initiated such a concept.

1.4DIGITAL SPACE AND FUNDAMENTAL FREEDOMS

Other basic freedoms and privacy human rights addressed in this context include freedom of speech, faith, political thought, poetry, and written texts; free and fair access to information; and the security of personal information such as family relationships, associations, and health information.[140] Furthermore, protected privacy from abuse and persecution on the Internet based on one's own political, ethical, or gender status, as well as undisclosed personal, educational, or health records, is a

[139]Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute. Available at: .

[140]Chinn, D., Kaplan, J. and Weinberg, A., 2014. Risk and responsibility in a hyperconnected world: Implications for enterprises, Report - January 2014. [online] Geneva: Word Economic Forum. Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/risk-andresponsibility-in-a-hyperconnected-world-implications-for-enterprises

cornerstone of human rights in cyberspace. Cyber human rights should protect an individual's intellectual property and creativity in areas such as art, movies, pictures, literature, scientific results, etc. with access at any time to fair and open trials. Good cyber governance has to be conducted over a domain of an individual's public privacy, which includes public and private data. It must strike a balance between Internet freedom of information and expression and the security and privacy of individuals in cyberspace. Privacy, according to international principles and concepts, is a personal space where we can confidently and freely grow our personalities, exercise our talents and abilities, protect our fitness, and enjoy social interactions with family and friends.As a result, using the Internet as a service medium for private reasons without fear of third parties, such as governments or businesses (e.g., national security services, Google+, Microsoft), accessing, selling, or openly posting our data for national security or commercial purposes without our permission is referred to as privacy in cyberspace.

Maintaining public privacy eventually faces the task of balancing our personal, technical, and private interests while providing norms and laws that may hinder any degree of privacy using the Internet as a free and open access communication platform. The debates and discussions around Internet freedom and privacy rightsare fundamentally important in the areas of data protection, cybersecurity, cyber surveillance, and cyberwar through computer viruses. Some call it the "World Wide War" in which various state and non-state actors such as individual hackers are equally involved. Commercial-state or inter-govern- mental agreements, such as the Stop Online Piracy Act (SOPA), the NSA's surveillance program, PRISM, or the Anti- Counterfeiting Trade Agreement (ACTA), are just a few governmental initiatives to regain the control over the borderless dataflow.

The problem would be determining if these frameworks and commitments will fully protect human rights. The often declared 'right to Internet,' which aims to include individual access to the Internet at any time, and the right to be forgotten, which ensures that one's own personal data remains private and can be deleted at any time, are already part of overall human rights standards concerning access to information, privacy, and data protection (as in the EU Fundamental Rights Charter) and participation. The EU Court of Justice passed a land- mark decision in May 2014 that but- tresses privacy and the right of users to have their data removed or forgotten from the Internet. The ruling targets search engines and data providers such as Google, YouTube, and Facebook. Unfortunately, it only applies to the EU territorial space. A global solution has yet to come.[141]

The European Court of Human Rights' Research Division made some progress in 2011 by releasing a landmark paper on future case law surrounding Internet-related privacy and retention problems. Other foreign or domestic courts, on the other hand, can take some time to interpret the legal rights established by the EU Court of Justice. Human rights are often inscribed and enforced by treaties, customary international law, general principles, and other sources of international law. Governments, corporations, persons, and other lawful bodies (duty bearers) have rights and responsibilities to behave in certain ways or refrain from certain actions. There is no hierarchy of human rights, which are sometimes referred to as social, legal, economic, political, or cultural rights. Without one another, these various types of human rights cannot be practiced or enjoyed.For example, the universal right to

[141]Proença, D., Vieira, R. and Borbinha, J., 2016. "A maturity model for information governance". In: International Conference on Theory and Practice of Digital Libraries. Cham: Springer, pp. 15-26.

access exists only where the information does not infringe on the integrity or privacy of others. This is the Golden Rule-based holistic approach to human rights: “Do not hurt others in the way that you may not want done to you.”In this vein, a cyber human rights regime should be calibrated and assessed insofar that it would not infringe on others’ rights.

That being said, protection of data should never justify censorship or random surveillance of individuals. Finding the balance depends very much on who decides the limits and borders of freedom of information. The greater the number of parties involved, the more likely the final balance would be agreed. Finally, in 2012, the United Nations Human Rights Council told us that human rights are applicable both online and offline, and that whether they are broken in cyberspace or in physical space across borders makes no difference. However, the issue of who is the duty bearer remains unanswered. Who will defend, execute, and uphold human rights in cyberspace if government authorities stop at state borders? In 3013, the issues of cyber espionage and misuse of private data came about through the NSA affair between the United States, Germany, and Brazil. The former NSA contractor, Edward Snowden, revealed the U.S. government’s warrantless and limitless surveillance of U.S. citizens and Internet users around the world.

The United States is now charging Snowden under the U.S. Espionage Act, but Snowden remains in exile in Russia while theU.S. government works on extradition. Snowden’ s revelations continue to strongly impact the debate about privacy and its insufficient legal development and heavily violated laws. Even though the UN, the EU, and many nations extensively fine-tuned their laws and regulations on data protection in 2013, the main issue remains unresolved: how can privacy and freedom rights be safeguarded in cyberspace, if at all? Individually, many users started to adapt and become more cautious.[142] Consequently, self- censorship by users could not be avoided and manysensitive communications no longer take place online. Facebook users have become alarmed at posting private pictures online, and millions of users no longer send their e-mails unencrypted. The need for technical tools such as encryption and deciphering technology are highly demanded. In Europe alone, the number of encrypted data transferred rose in 2014 from 1.5% to 6.0%. Yet overall Snowden’s revelations demonstrated that the problems of global surveillance - conducted by most NSAs in this world - need global answers, not just national or regional ones, let alone technical ones. The many national laws passed over the past year regarding data protection can only create more time, but not deliver the solution. Meanwhile, private, governmental and non governmental actors have to discuss and decide which will be the common cyber- rules, standards and governance mechanisms that will end anarchy in cyberspace in the near future. In response to these and other revelations, the UN Special Rapporteur on Freedom of Expression Frank de la Rue highlighted the fact that privacy and freedom of expression are interlinked and mutually dependent.

As a result, without adequate legislation and legal standards to ensure the privacy, security, and anonymity of communications journalists, human rights defenders, and whistleblowers, it is impossible to ensure that their communications will not be subject to states’ security uses.” Jon Perry Barlow wrote the “Declaration in

[142]Sonmez, M. and Yildırım, S., 2015. “A Theoretical Aspect on Corporate Governance and Its Fundamental Problems: Is It a Cure or Another Problem in the Financial Markets?”. Journal of Business Law and Ethics, [online] Volume 3 (No. 1 & 2), pp. 20-35. Available at: http://jblenet.com/journals/jble/Vol_3_No_1_June_2015/2.pdf

Independence of Cyberspace" in 1996, describing the situations and controversies that today's Internet users are concerned with around the world.Barlow realized twenty years ago that the Internet world, and therefore the global consumer community, needed to create their own social contracts and figure out how to deal with their challenges based on the Golden Rule, which is the basis for realizing human rights. Whether or not such cyberspace social contracts are ever implemented, the concept underlying them is personal responsibility and commitment to human rights, which we, as members of the global community (private or public), have long subscribed to. So-called 'digital rights' are already embedded in freedom rights, such as those stated in the Universal Declaration on Human Rights (UDHR) or the International Covenant on Civil and Political Rights (ICCPR). These rights allow the access and use of information and communications technology, like computers and digital media, to enhance any of the aforementioned human rights and the overall human right to information.[143] As a result, on December 10, 2013, the 65th anniversary of the UN's proclamation of the Universal Declaration of Human Rights, over 500 authors and Nobel Laureates signed a petition asking the UN to draft an international bill on digital rights. The user community's overwhelming enthusiasm for such a proposal is anticipated to have an effect on the advancement of global Internet governance concepts.

1.5 LET'S SUM UP

Governance, ultimately, human rights -oriented cyber governance is a new trend in which global Internet users aim to uphold their basic human rights through good cyber- governance principles. Yet there is no global rule of law culture in cyber-space as of yet, let alone any monitoring or enforcement mechanism based on the multi-stakeholder approach that would safeguard the rights of development towards an open and fair cyber governance regime.

1.6FURTHER READING

- A. Mihr (2013) Public Privacy-Human Rights in Cyberspace, Working Paper, Utrecht University.
- MindaugasKiskis (2011) Entrepreneurship in Cyberspace: What do we know?, Social Technologies, MykolasRomeris University, I (i), 37~4
- Internet Governance Forum Helen Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology (1997) 7 (3)» Ethics & Behavior, 207-219.
- Court of Justice of the European Union (May 2014), Factsheet about Right to be Forgotten ruling C 131/12 .

[143]ITU, 2008. Overview of cybersecurity, ITU-T X.1205. [online] Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I/en

1.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Why is Human-based rights approach needed for Good Cyber Governance?

Through the use of cyber technologies such as the Internet and mobile devices, good cyber governance must create a human rights-based strategy for (1) more openness, (2) more openness, and (3) more stakeholder involvement. Furthermore, good cyber governance promotes and protects human rights through technology. Cyberspace, though, is a borderless public space in which people, regardless of their citizenship, race, sex, political affiliation, or gender collaborate and connect.

1.8ACTIVITY

Elaborate the fundamental freedoms in digital space which should be protected. (800-900 words)

Unit 2: PRIVACY AND DATA PROTECTION: AN INTERNATIONAL PERSPECTIVE

2

Unit Structure

2.1 Learning Objectives

2.2 Introduction

2.3 Conceptualisations of Privacy and Related

2.4 Conceptualisations of the Values Served by Privacy

2.5 Societal and Cultural Support for Privacy

2.6 Let's sum up

2.7 Further reading

2.8 Check your progress: Possible Answers

2.9 Activity

2.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- privacy provisions of various countries
- data protection of the individuals
- data protection and privacy

2.2 INTRODUCITON

This chapter examines the establishment of legislative instruments (statutes, recommendations, guidance, and so on) to protect privacy and related interests in the collection of personal data across jurisdictions.In Europe, such instruments are commonly referred to as “data security” instruments, which is also the nomenclature used in this chapter. Defense of “privacy,” “personal privacy,” or “information privacy” is the preferred nomenclature outside of Europe. Regardless of these terminological distinctions, all of the instruments constituting the subject of this chapter are expressly aimed at restricting the collection of data relating to, and promoting recognition of, individuals (i.e., personal data) in order to preserve, at least partially, the privacy and related interests of those persons.[144]
The central rules that are applied to the processing of such data herein embody a set of mostly procedural, “fair information” principles stipulating, among other things, the manner and purposes of data processing, measures to ensure adequate data quality, and measures to ensure that the processing is transparent to, and influenced by, the individual to whom the data relate (“data s”). These instruments, when taken together, constitute an area of law and policy that has grown in sophistication, spread, and normative significance over the last four decades.[145]About forty countries have already adopted data privacy legislation that is reasonably robust. A vast variety of international agreements supplement and also inspire these national programs. An enormous body of scholarly commentary envelops the regulatory sector, analyzing privacy and data security topics from a range of viewpoints. As a result, the global data security landscape is extremely complex, and it is beyond the reach of this chapter to adequately represent all of its nooks and crannies.

2.3CONCEPTUALISATIONS OF PRIVACY AND RELATED INTERESTS

Privacy is a hot topic of discussions regarding the social and political dangers raised by new information and communications technologies (ICT). This is especially true in the United States of America (USA), where the term “privacy” is commonly used in cultural, scholarly, and legal debate. When significant debate began in the 1960s over the effects of computerized collection of personal records, the word “privacy” was coined as a catch-all term for the slew of concerns posed by the (mis)use of

[144]See generally Regan, P.M., Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, Chapel Hill / London 1995.
[145]See, e.g., Westin, A.F., Privacy and Freedom, Atheneum, New York 1970; Miller, A., The Assault on Privacy: Computers, Data Banks and Dossiers, University of Michigan Press, Ann Arbor 1971.

machines. However, protection is not the only word that has been used in this way. Other, partially overlapping terms, such as “democracy,” “liberty,” and “autonomy,” have also been mentioned.[146] The debate in the United States, especially in the 1960s and early 1970s, about the privacy challenges faced by modern ICT had a significant impact on debates in other countries. “Almost every issue that arose in Europe was also an issue in the United States, but at a much earlier time and on a much larger scale,” writes Hondius.

The importance of the privacy principle in American discourse contributed to its popularity in other debates. This is most noticeable in English-speaking countries and international forums where English is used as a working language. And in countries where English is not the primary language, much of the same debate has been framed, at least at first, around definitions that are loosely equivalent to, or embrace, the principle of privacy.Nonetheless, the area of law and policy that arose from early European discussions about the privacy risks faced by ICT has often been defined using a nomenclature that avoids overt references to the words “privacy” and “privacy-related terms.” The expression “data security” is derived from the German word “Datenschutz.” While the nomenclature is flawed in many ways, including failing to indicate the core interests represented by the standards to which it is intended to refer, it has achieved widespread acceptance in Europe and, to a lesser degree, elsewhere. However, the word “data protection” is gradually being used in its place. The latter term is potentially more fitting than “data security” because it better communicates the core issue(s) at hand and serves as a link between North American and European policy debates.However, it would be a mistake to presume that the terms “data security” and “privacy” are interchangeable. They are not similar, at least from a European perspective, despite their close relationship. The term “data security” is usually used to refer to a collection of rules that cover a wider spectrum of concerns than just privacy. And the degree that such conventions address privacy rights, they only address the informational aspects of privacy rather than the spatial or physical dimensions.

Various countries and territories have their own terminological quirks, which are partially due to varying jurisprudential contexts for the debates in question.[147] The debate in Western Europe has often relied on the region’s jurisprudence on legal identity rights. As a result, the definitions of “Persönlichkeitsrecht” and “Persönlichkeitschutz” play a central role in German and Swiss data security debate. The principle of “personvern” (“protection of person(ality)”) dominates Norwegian discourse, while “integritetsskydd” (“protection of (personal) integrity”) dominates Swedish discourse.[148]Latin American debate in the region, on the other hand,

---

[146]See, e.g., United Kingdom, Committee on Privacy (the Younger Committee), Report of the Committee on Privacy, Cm. 5012, Her Majesty’s Stationery Office, London 1972; Canada, Department of Communications and Department of Justice, Privacy and Computers: A Report of a Task Force, Information Canada, Ottawa 1972; Australian Law Reform Commission, Privacy, Report no. 22, Australian Government Publishing Service, Canberra 1983; Morison, W.L., Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys-General, Report no. 170/1973, Australian Government Publishing Service, Canberra 1973.

[147]See, e.g., Hughes, G.L. and Jackson, M., Hughes on Data Protection in Australia, Law Book Co. Ltd., Sydney 2001, 2nd ed.

[148]See, e.g., Guadamuz, A., Habeas Data: The Latin American Response to Data Protection, The Journal of Information, Law and Technology 2000, no. 2, “www2.warwick.ac.uk/ fac/soc/law/elj/jilt/2000_2/guadamuz”; Organization of American States (O.A.S.), InterAmerican Juridical Committee (rapporteur Fried, J.T.), Right to Information: Access to and Protection of Information and Personal Data in Electronic Form, in Annual Report of the Inter-American Juridical Committee, CJI/doc. 45/00, p. 107 et seq. While the concept originates in South

continues to revolve around the definition of “habeas data” (roughly translated as “you should have the data”). Due-process doctrine, which is founded on the writ of habeas corpus, gives rise to this definition. Many of the definitions listed above are subject to definitional inconsistency. The most well-known example is “privacy.” Various meanings of the term abound, and a lengthy – yes, a lengthy – controversy has erupted, mostly in American circles, over which meaning is the most accurate. Parallel discussions on related concepts can be seen in other nations, but they tend to be somewhat less robust than the privacy debate. Any of the above controversy revolves around whether privacy should be classified as a state, a claim, or a privilege. Aside from that, the controversy exposes four major definitions of privacy. One collection of meanings is based on non-interference, while another is based on restricted access. A third group of concepts considers privacy to be the ownership of content.

A fourth set of meanings combines concepts from the other three sets, but only applies to private or important facets of people’s lives. Not unexpectedly, concepts of privacy in terms of information security are most common in discussions of data protection law and policy. Most of the debate, both in the United States and abroad, revolves around the concept of access management. However, in Europe, the term is not necessarily immediately connected to the concept of privacy; it is either linked to similar terms such as “personal dignity” (as in Swedish discourse) or it stands alone.The German concept of “information self-determination” (“informationelleSelbstbestimmung”), which is the substance of a constitutional right derived from a historic ruling by the German Federal Constitutional Court in 1983, is the most notable example of the above (Bundesverfassungsgericht). The concept, as well as the right attached to it, has had a significant effect on the advancement of data protection law and policy in Germany and, to a lesser degree, other European countries.Despite their widespread acceptance, concepts of knowledge ownership and self-determination have seldom been interpreted in terms of an individual “owning” information about himself or herself, so that he or she may be entitled to royalties for its use by others. Property rights doctrines, on the other hand, have rarely been championed as a desirable foundation for data protection rules. The few advocates of a property rights approach have appeared to come from the United States, but there has been some scattered activism internationally.[149]

2.4CONCEPTUALISATIONS OF THE VALUES SERVED BY PRIVACY

What are the ideals supported by respect for privacy as described by different nations or cultures? Is anonymity, for example, perceived as primarily (or exclusively) of importance to individuals or as having wider societal benefits? In the United States, much discussion of privacy and privacy protection focuses only on the benefits of people as individuals. Individuality, integrity, integrity, emotional freedom, self-evaluation, and inter-personal relationships of affection, friendship, and trust are usually cast in terms of securing (or helping to secure) individuality, autonomy,

America, it has also begun to gain a foothold in parts of South-East Asia. In 2008, the Supreme Court of the Philippines formally adopted a “Rule on the Writ of Habeas Data” as a Rule of Court.

[149]See, e.g., Warren, S.D. and Brandeis, L.D., The Right to Privacy, Harvard Law Review 1890, vol. 4, p. 193, 205 (arguing that the right to privacy in Anglo-American law is part and parcel of a right “to be let alone”).

dignity, emotional release, self-evaluation, and inter-personal relationships of love, friendship, and trust.[150] They are primarily about "achieving individual goals of self-realization," as Westin puts it.The flip side of this focus is that privacy and privacy protection are often seen as being in direct conflict with the interests of a larger "society." This viewpoint is often expressed in arguments that privacy rights are incompatible with social needs.

Casting the value of privacy in purely individualistic terms continues to be a prevalent feature of many other countries' equivalent debate. Indeed, it is a key component of what Bennett and Raab refer to as the "privacy model" – a series of liberal assumptions that guides the implementation of data security policy in the vast majority of advanced industrial countries. Despite this, the paradigm's hold ranges from country to country and culture to culture. When comparing the German Federal Constitutional Court's jurisprudence to that of US courts, the differences are clear.[151]The former emphasizes that the importance of data security norms is largely determined by their capacity to provide the requisite conditions for active citizen participation in public life; in other words, to ensure a healthy democracy. In American law, this viewpoint is underdeveloped. We're also seeing a growing awareness in intellectual debate on both sides of the Atlantic that privacy and data security norms are important not only for individuals, but also for the preservation of societal civility, pluralism, and democracy.

A related trend is the growing awareness by academics that data security laws represent a variety of needs, some of which go far beyond conventional notions of privacy. This understanding has probably progressed the most in Norwegian debate, which has established relatively sophisticated models of the different interests supported by data protection laws. Ensure sufficient quality of personal records, "citizen-friendly" government, proportionality of power, and the rule of law are among these interests.The realization that data security policies are about more than protecting privacy has spread beyond academia and into regulatory bodies in Norway. Indeed, in addition to the needs for anonymity and personal dignity, Norway's main law on the subject includes an objects provision expressly relating to the requirement for "adequate quality of personal knowledge." Any other European countries' equivalent regulations have objects provisions that cover more than just privacy.The French legislation expresses the broadest, if not the most audacious, set of goals: "Information technology should be at the service of every citizen." It will be established in the sense of international collaboration. It must not infringe on people's identities, rights, privacy, or personal or public liberties." Also notable is the explicit concern expressed in many German Länder' early data security laws for preserving State order based on the principle of division of powers, as well as

[150]Laudon, K.C., Markets and Privacy, Communications of the Association for Computing Machinery 1996, vol. 39, p. 92–104; Lessig, L., Code and Other Laws of Cyberspace, Basic Books, New York 1999, p. 159–162; Rule, J.B. and Hunter, L., Towards Property Rights in Personal Data, in Bennett, C.J. and Grant, R. (eds.), Visions of Privacy: Policy Choices for the Digital Age, University of Toronto Press, Toronto 1999, p. 168–181; Rule, J.B., Privacy in Peril, Oxford University Press, Oxford 2007, p. 196–198. Cf. Schwartz, P.M., Property, Privacy, and Personal Data, Harvard Law Review, 2004, vol. 117, p. 2056–2128 (critically discussing various objections to a property approach but ultimately arguing in favour of a qualified "propertization" of personal data).

[151]See, e.g., Blume, P., New Technologies and Human Rights: Data Protection, Privacy and the Information Society, Paper no. 67, Institute of Legal Science, Section B, University of Copenhagen 1998.

ensuring so-called “data equilibrium” (“Informationsgleichgewicht”) between the legislature and other State institutions.[152]This “equilibrium” applies to a situation in which the legislative is able to obtain information (personal and/or non-personal) that the executive has access to. In certain nations, however, there is some confusion about the rights and principles are promoted under data protection legislation. This is expressed in scholarly debate, in the fact that certain statutes lack objects clauses that formally define the specific objectives or principles that the statute is meant to represent, and in the frequently ambiguous manner in which modern objects clauses are drafted.[153]

2.5SOCIETAL AND CULTURAL SUPPORT FOR PRIVACY

Making fair assessments of the degree to which different nations or societies value privacy is challenging – a challenge that clearly extends to comparing the regulatory regimes for privacy and data security of different countries. This challenge stems in part from a lack of systematically collected scientific evidence, and in part from the fact that privacy concerns vary widely across countries and cultures.Proposals to introduce multi-purpose Personal Identification Number (P.I.N.) schemes similar to those in Scandinavia, for example, have traditionally been met with strong opposition in the United Kingdom (U.K.),[154] despite the fact that video surveillance of public places in the U.K. appears to be far more extensive than in Scandinavian countries, and indeed the rest of the world. The level of privacy varies greatly across nations and societies, as well as across long stretches of time.Furthermore, the ways in which people establish, protect, and improve their respective states of privacy, as well as the degree to which they express a preference for privacy, differ from culture to culture due to a variety of reasons. Around the same moment, the need for secrecy continues to be a universal human characteristic. Human beings seem to follow different techniques for cultivating other types of social distance including in communities where physical or spatial solitude appears to be restricted.[155]
If there is a panhuman desire for anonymity, it tends to be embedded in social rather than physiological or biological considerations. According to Moore, the desire for privacy is primarily a social construct. Moore’s groundbreaking study suggests that an extensive, deeply established respect for privacy is only possible in a comparatively dynamic society with a firmly felt distinction between a domestic private domain and public sphere “privacy is limited where technology and social organisation are restricted”. However, technical and corporate considerations aren’t the only factors that influence privacy levels.Cultural, moral, and metaphysical

[152]See Bennett, C.J. and Raab, C.D., The Governance of Privacy. Policy Instruments in Global Perspective, M.I.T. Press, Cambridge, Massachusetts 2006, 2nd ed., chapt. 1.
[153]See, e.g., Schwartz, P.M., The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, American Journal of Comparative Law 1989, vol. 37, p. 675–701; Ruiz, B.R., Privacy in Telecommunications: A European and an American Approach, Kluwer Law International, The Hague / London / Boston 1997; Eberle, E.J., Dignity and Liberty: Constitutional Visions in Germany and the United States, Praeger, Westport, Connecticut 2002, p. 88–94.
[154]See, e.g., the U.K. Data Protection Act of 1998 and Denmark’s Personal Data Act of 2000 (Lovnr. 429 af 31. maj 2000 om behandlingafpersonoplysninger).
[155]see, e.g., Lunde, A.S., Huebner, J., Lettenstrom, G.S., Lundeborg, S., Thygesen, L., The Person-Number Systems of Sweden, Norway, Denmark and Israel, U.S. Department of Health and Human Services; Vital and Health Statistics : Series 2 ; no. 84; D.H.H.S. Publication No. (P.H.S.) 80-1358, Washington, D.C. 1980.

influences all play a role. Attitudes toward the importance of private life, attitudes toward the worth of people as individuals, and attention to noneconomic and emotional needs of people are all important. In cultures that espouse political values, such as those of Mill, Locke, Constant, and Madison, privacy is a major concern. As Lukes points out, privacy is "probably the fundamental concept of liberalism" in the context of a "sphere of thinking and action that should be free from 'public' intervention."[156]

The liberal love for privacy is evident in the establishment of privacy-protection legal frameworks. Western democracies have the most comprehensive regimes. In most African and Asian countries, on the other hand, such regimes remain underdeveloped. It's tempting to see this situation as symptomatic of African and Asian cultures' proclivity for prioritizing the group's desires and loyalties at the detriment of the citizen. However, it is important to avoid categorizing countries and cultures into rigid groups.

2.6 LET'S SUM UP

The differences between the different data security regimes are also highlighted in this chapter. As a result, it is appropriate to conclude with a few short observations on the prospects for greater global harmonisation of regulatory regimes. To put it bluntly, comprehensive economic harmonisation is incredibly difficult to happen anytime soon. This is due in part to the global strength of entrenched ideological/cultural disparities.As previously stated, such divisions exist even within representatives of the Western, multicultural, democratic sphere, and they will not go away easily. Future foreign policymaking in the region will have to negotiate seriously with nations and communities outside of the sphere, which will make bridging gaps much more difficult. Another consideration is the absence of a solid, dynamic, and representative international body capable of bridging the gap.

2.7FURTHER READING

- Reidenberg, J.R., Resolving Conflicting International Data Privacy Rules in Cyberspace, Stanford Law Review, 2000, vol. 52, p. 1315–1371.
- Rossnagel, A., Pfitzmann, A., Garstka, H., Modernisierung des Datenschutzrechts, report for the German Federal Ministry of the Interior (Bundesministerium des Innern), September 2001.
- Regan, P.M., Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, Chapel Hill / London 1995.

[156]See, e.g., Moore, B., Privacy: Studies in Social and Cultural History, M.E. Sharpe, New York 1984; Roberts, J.M. and Gregor, T., Privacy: A Cultural View, in Pennock, J.R. and Chapman, J.W. (eds.), Privacy: Nomos XIII, Atherton Press, New York 1971, p. 199–225; Altman, I., Privacy Regulation: Culturally Universal or Culturally Specific?, Journal of Social Issues 1977, vol. 33, p. 66–84.

- Hughes, G.L. and Jackson, M., Hughes on Data Protection in Australia, Law Book Co. Ltd., Sydney 2001, 2nd ed.
- Solove, D., Understanding Privacy, Harvard University Press, Cambridge, Massachusetts 2008, chapters 1–2.
- Inness, J.C., Privacy, Intimacy, and Isolation, Oxford University Press, New York / Oxford 1992, chapter 2.

2.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Which country has used boldest approaches while formulating data privacy laws?**

   The French law expresses the broadest, if not the most audacious, set of goals: “Information technology should be at the disposal of any citizen.” It will be established in the sense of international collaboration. It does not infringe on people’s identities, rights, anonymity, or personal or public liberties.”

2.9 ACTIVITY

Elaborate the measures used for facilitating identification of persons (i.e., personal data) in order to safeguard the privacy and related interests of those persons.

3

Unit 3: EUROPEAN DATA PRIVACY LAW DEVELOPMENTS

Unit Structure

3.1 Learning Objectives

3.2 Introduction

3.3 Adoption of The General Data Protection Regulation

3.3.1. Territorial Scope
3.3.2. Personal Data Processing Principles
3.3.3. Legitimate Processing Bases, Including Consent
3.3.4. Data-Subject Rights

3.4 The Privacy Shield

3.5 Google and The Right To Delisting

3.6 Let's sum up

3.7 Further reading

3.8 Check your progress: Possible Answers

3.9 Activity

3.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- General data protection regulation
- Personal data processing principles
- Natural person's right to delist from search engine
- Privacy shield

3.2 INTRODUCTION

Some of the most significant European data privacy law developments that have emerged since the European Union adopted the Data Protection Directive in 1995 occurred in the year 2014. These include the adoption of the European Union's General Data Protection Regulation ("GDPR"), the invalidation by the Schrems decision of the U.S.–EU Safe Harbor cross-border data-transfer framework, and the subsequent replacement of the Safe Harbor framework with the EU-U.S. Privacy Shield. The "right to delisting," which the 2014 Google Spain decision created, also experienced continued development. This survey reviews the GDPR's main provisions—arguably the most important recent development - and then discusses the other developments noted above.[157]

3.3ADOPTION OF THE GENERAL DATA PROTECTION REGULATION

On April 27, 2016, the European Union finally adopted the GDPR, more than four years after the European Commission proposed it. The regulation came into force on May 24, 2016 and it will become applicable starting May 25, 2018 when it will repeal the current Data Protection Directive. This gives companies until May 2018 to adapt to its new provisions.[158]

European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as "data subjects," with respect to their personal data processing. The GDPR defines both "processing" and "personal data" broadly and in adherence with the Data Protection Directive, even though it reorganizes and updates the Data Protection Directive's definitions.[159] Processing with respect to personal data may include, but is not limited to, the

[157]Voss, W.. (2017). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. Business Lawyer, The. 72. 221.

[158]Dove, Edward. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics. 46. 1013-1030. 10.1177/1073110518822003.

[159]Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

following: “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, era- sure or destruction.” The relevant personal data are” any information relating to an identified or identifiable natural person (‘data subject’),” and may include location data, online identifiers, and other forms of information that may be used to identify a data subject directly or indirectly, in addition to classic identifying data such as names and identification numbers.
The following sections address a few of the GDPR provisions that differ significantly from the Data Protection Directive and are important for businesses.

3.3.1TERRITORIAL SCOPE

The GDPR’s territorial scope is larger than that of the Data Protection Directive. The personal data processing place no longer controls the analysis; instead, under the GDPR, processing merely must occur “in the context of the activities of an establishment of a controller or a processor in the Union,” a definition that expands the analysis to include the activities of the processor that processes personal data on behalf of the data controller.[160] The GDPR also applies to the “pro- cessing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union” so long as the processing is related to “the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union” or the monitoring of such data subjects’ behavior “as far as their behaviour takes place within the [European] Union.” For example, the GDPR applies to a U.S. provider’s cloud-based-services offering to individuals in the European Union, even where the offering requires no payment and the provider has no establishment in the European Union, to the extent that the offering involves processing those individuals’ personal data.[161]

3.3.2PERSONAL DATA PROCESSING PRINCIPLES

Although the GDPR’s personal data processing principles are similar to those in the Data Protection Directive, there are a few differences. For example, the GDPR explicitly requires data to be processed “in a transparent manner,” but the Data Protection Directive only implicitly requires transparency.[162] In addition, the GDPR specifies that in accurate data must be erased or rectified “without delay,” adding a time element to the “accuracy” principle already contained in the Data Protection Directive.[163] Finally, the “accountability” principle requires the controller to be able to

[160]GDPR, supra note 3, art. 99(1), at 87 (“This regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.”). The date of its publication in the Official Journal of the European Union was May 4, 2016.
[161]GDPR, supra note 3, art. 4(1), at 33. Compare Directive 95/46, supra note 1, art. 2(a), at 38 (defining “personal data”).
[162]GDPR, supra note 3, art. 3(1), at 32. Compare Directive 95/46, supra note 1, art. 3, at 39 (addressing scope). The consideration of a processor’s activities in determining the territorial scope of the GDPR reflects the greater accountability of processors under the GDPR, when compared to the Data Protection Directive.
[163]GDPR, supra note 3, art. 5(1)(a), at 35 (“processed lawfully, fairly and in a transparent manner”). Compare Directive 95/46, supra note 1, art. 6(1)(a), at 40 (“processed fairly and lawfully”).

demonstrate compliance with the other personal data processing principles. This latter provision ties into the new GDPR record- keeping obligations discussed in Section II.G.

3.3.3LEGITIMATE PROCESSING BASES, INCLUDING CONSENT

The GDPR retains the requirement that a legitimate basis must exist in order for personal data processing to be lawful. It further develops the "purpose limitation" principle, allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject's consent. This compatibility determination considers, among other things, links between the two purposes, context (including the relationship between the data subject and the controller), the data's nature (specifically, whether special data categories are involved), possible consequences for the data subject, and the existence of "appropriate safeguards," which could include data encryption orpseudonymization.[164]

Where consent is the processing basis, it must be unambiguous. The Data Protection Directive provided that "the data subject's consent" meant "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." The GDPR similarly defines data subject "consent" but provides the additional requirement that the data subject's wishes be "unambiguous" and manifested "by statement or by a clear affirmative action."

The GDPR sets out additional conditions for such consent beyond those contained in the Data Protection Directive, including a requirement that the controller be able to demonstrate that the data subject has given his or her consent. If a declaration that covers other matters contains a consent request, the request must be clearly written and distinguishable from those matters, with one risk for non-compliance being that the declaration's consent request will be non- binding. These requirements encourage good recordkeeping and proper document drafting.

3.3.4DATA-SUBJECT RIGHTS

The GDPR requires transparency in the provision of information to data subjects about their rights and the means of exercising them. This requirement applies regardless of whether data are collected directly from the data subject or indirectly from a third party. Under the GDPR, data subjects continue to benefit from rights they had under the Data Protection Directive, such as the right to access, the right to object to processing (which they may exercise at any time when the processing is for direct-marketing purposes), and from the transparency-and accuracy-principle requirements discussed above, as well as the related right to rectification "without

[164]Compare Directive 95/46, supra note 1, art. 7(f), at 40 ("[P]ersonal data may be processed only if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party . . . .") (emphasis added).

undue delay."[165] A data subject has the right not to be subject to a "decision based solely on automated processing including profiling, which produces legal effects concerning him or her or significantly affects him or her," subject to certain exceptions, such as where the data subject provides explicit consent or where automated processing is necessary for a contract between the controller and the data subject.

The GDPR creates several new rights for data subjects beyond those provided by the Data Protection Directive. First, it creates a "[r]ight to erasure ('right to be forgotten')." This right is often dependent on the data subject meeting the criteria set out in the relevant clause (e.g., it is subject to there being no overriding legitimate grounds for the processing, where the data subject exercises his or her right to object to it), and may become inapplicable where processing is necessary for exercising the right of freedom of expression and information, for certain reasons based on the public interest, or for establishing, exercising, or defending legal claims. Furthermore, "taking account of available technology and the cost of implementation," a controller that has made data public before being required to erase it shall take "reasonable steps . . . to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of such data.

Moreover, a right to restrict processing may apply, either for a period of time for purposes set out in Article 18 of the GDPR, or as an alternative to data era- sure. The GDPR also creates a right to data portability, which allows data subjects to request the controller to return their data in a commonly used, machine- readable format, and to request that the controller transmit such data to another controller if the processing was based on consent and was carried out by auto- mated means. The right does not apply to processing that was necessary for public interest or official authority tasks, and it must not "adversely affect the rights and freedoms of others."[166]

Finally, European Union or Member State law may restrict certain data subject rights when the restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard, among other things, national security, defense, the fight against crime, and the furtherance of justice.

3.4THE PRIVACY SHIELD

The European Commission/DoC negotiations led to the establishment of the "EU–U.S. Privacy Shield" and the corresponding European Commission draft adequacy decision. Attached to the draft adequacy decision are seven annexes from U.S. government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations.[167] One improvement from a data subject perspective is greater opportunity for recourse through an independent recourse mechanism provided by the data controller. In addition, under

[165]Compare Directive 95/46, supra note 3, art. 12, at 42

[166]GDPR, supra note 3, art. 17(1)(c), at 44.

[167]Mark Scott, In Europe-U.S. Clash on Privacy, a Longstanding Schism, N.Y. TIMES (Oct. 7, 2015), http://nyti.ms/1Q93iJM.

this new frame work, an individual data subject may invoke binding arbitration of claims pursuant to the Privacy Shield principles under certain conditions. Furthermore, the Federal Trade Commission ("FTC") will review non-compliance allegations "to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated," potentially resulting in enforcement action under the FTC Act. Moreover, the DoC has committed to providing greater oversight and Privacy Shield compliance monitoring.[168]
Following data protection authority comments, the parties modified the EU-U.S. Privacy Shield to include "additional clarifications on bulk collection of data, strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers,"[169] and they adopted the final implementing decision with revised annexes. The Privacy Shield became operational on August 1, 2016.

3.5GOOGLE AND THE RIGHT TO DELISTING

In the 2014, Google Spain case, the court granted a natural person the right to compel delisting of newspaper pages containing information prejudicial to him when Internet users searched for his name using a search engine. Google sought to limit the right's geographic scope to European web domains, while the French data protection authority ("CNIL") sought to have the delisting extended to all relevant domains including ".com."[170] The CNIL issued an order to that effect, which Google contested, prompting the CNIL to commence a formal procedure against it.
On March 10, 2016, the CNIL Restricted Committee imposed a €100,000 fine on Google. In doing so, it rejected Google's offer that it would "filter results based on the geographic origin of the person performing the search," meaning that "people using the search engine from the same country [as] the plaintiff's country [could] not access the delisted result anymore." The CNIL commented that "[o]nly delisting on all of the search engine's extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold" the right to privacy. Google announced that it was appealing the decision to the highest French administrative court.

3.6 LET'S SUM UP

The European Union has finally adopted data protection law reform, and now is the time for companies to adapt to the new landscape before the GDPR applies in May

[168]See European Commission Unveils EU-U.S. Privacy Shield, EUR. COMM'N (Feb. 29, 2016), http:// ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm.
[169]Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) [hereinafter Draft Commission Implementing Decision], http://ec. europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.
[170]See Commission Implementing Decision of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EUU.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) and Annexes 1 to 7, http://ec.europa.eu/ justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf and http://ec.europa.eu/ justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

2018. Many of the GDPR's provisions address companies' compliance obligations and require greater accountability and recordkeeping. Some provisions may require changes to internal organization (e.g., DPOs, DPIAs, and procedures that allow for proper data breach notifications). The United Kingdom's DPA issued a checklist of steps to prepare for the GDPR. These include raising awareness, documenting held personal data, reviewing privacy notices to bring them into conformity with the GDPR, checking that procedures cover all data subject rights and adapting them to cover handling data subject requests, identifying legal bases for processing, implementing systems to verify ages of children and to gather parental or guardian consent, implementing procedures regarding data breaches, designating DPOs if required, and identifying any applicable supervisory authorities.
With respect to cross-border personal data transfers, companies may now self-certify under the Privacy Shield. They should monitor developments regarding the right to delisting, as this affects access to information on the Internet.
In conclusion, it is clear that EU data protection and privacy law reform over the past year will necessarily require adaptation by companies and others for years to come.

3.7FURTHER READING

- Press Release, Eur. Comm'n, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016).
- CouncilDirective95/46,1995O.J.(L281)31(EC)[hereinafterDirective95/46].
- Case C-131/12, Google Spain SL v. AgenciaEspan˜ ola de Proteccio´n de Datos (AEPD), 2014E.C.R. 317,

3.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Why did the need for adoption of The General Data Protection Regulation arise?**

   European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as "data subjects," with respect to their personal data processing.

3.9 ACTIVITY

Elucidate the principles adhered to while adopting The General Data Protection Regulation. (1000-1500 words)

4

Unit 4: REGULATORY POLICY ON DATA PROTECTION

4.1 Learning Objectives
4.2 Introduction
4.3 International Instruments
4.4 Relative Impact of Regulatory Regimes
4.5 Let's sum up
4.6 Further reading
4.7 Check your progress: Possible Answers
4.8 Activity

4.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- International Instruments on Data Protection
- Impact of Data Protection regulatory regimes
- National Data Protection regimes in Europe

4.2 INTRODUCTION

This section provides an overview of the main legal instruments at both international and national levels which deal directly with data protection. Some account is also taken of instruments which formally are not legally binding but are, nevertheless, highly influential in development of regulatory policy in the field. Many, if not most, countries' legal regimes contain a multitude of laws that reflect aspects of the fundamental principles usually found in data security instruments or that may otherwise facilitate the realization of these principles, but in haphazard, ad hoc ways. Data protection, breach of trust, slander, and intellectual property laws are only a few examples. The following review is largely concerned with the extent to which countries have implemented rule-sets that are explicitly dealing with fostering data security.The extent to which countries allow for the creation of autonomous bodies (hereinafter referred to as "data protection authorities") expressly tasked with monitoring the enforcement and/or further advancement of these rule-sets is also of primary concern.[171]

4.3INTERNATIONAL INSTRUMENTS

The formal normative basis for data protection laws derives mainly from catalogues of fundamental human rights set out in certain multilateral instruments, notably the Universal Declaration of Human Rights (U.D.H.R.), the International Covenant on Civil and Political Rights (I.C.C.P.R.) along with the main regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (E.C.H.R.) and the American Convention on Human Rights (A.C.H.R.). All of these instruments – with the exception of the African Charter on Human and People's Rights – expressly recognise privacy as a fundamental human right. The omission of privacy in the African Charter is not repeated in all human rights catalogues from outside the Western, liberal-democratic sphere. Individuals have a right to privacy, according to the Cairo Declaration on Human Rights in Islam (see Article 18(b) – (c)). Other civil rights, such as freedom from oppression and freedom of speech, are also applicable in these instruments, while the right to privacy is closely tied to the values and concepts of data protection legislation.[172] The fact that

[171]MeitY, Feedback on Draft Personal Data Protection Bill, available at https://meity.gov.in/content/feedback-draft-personal-data-protection-bill.

[172]Park, Sungmi&Akatyev, Nikolay & Jang, Yunsik& Hwang, Jisoo& Kim, Donghyun& Yu, Woonseon& Shin, Hyunwoo& Han, Changhee& Kim, Jonghyun. (2018). A comparative study on data protection legislations and

data protection policies often point out protection of that right as fundamental to their formal logic reflects the particular value of the right to privacy in this sense. It is also reflected in case law developed pursuant to I.C.C.P.R. Article 17 and E.C.H.R. Article 8: both provisions have been authoritatively construed as requiring national implementation of the basic principles of data protection laws with respect to both the public and private sectors.[173]

In reality, these laws serve as data security instruments in and of themselves. However, case law is yet to enforce them in terms that greatly expand on the standards already present in other data security laws, and the defense they actually provide falls short of that provided by many of the latter instruments in several cases. There is no genuinely universal agreement or protocol dealing directly with data security in all international legal instruments. Calls for such an instrument are increasingly made, and work is underway to draft an appropriate set of international rules on point. Yet while there is clearly a need for a global legal approach in the field, there is, realistically, scant chance of, say, a U.N.-sponsored convention being adopted in the short term. The closest to such an instrument at present is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "C.o.E. Convention"). Although this is a European instrument, it is envisaged to be potentially more than an agreement between European states as it is open to ratification by states not belonging to the Council of Europe, though only upon the Council's invitation (see Article 23).[174] Civil society representatives have recently pushed to get non-member states to take advantage of this possibility though it is too early to tell whether this initiative will bear fruit. At present, the Convention has yet to be ratified by a non-member state. As for the E.U., its constitutional instruments now recognise that protection of personal data is in itself (i.e., separate from the broader right to privacy) a basic human right. This is a significant and hitherto unique development at the international level.

The main international conventions concerned directly with data security seek to encourage not only the enactment but also the harmonisation of national laws. The harmonisation goal has many justifications, some of which are less concerned with data security and more concerned with promoting the exchange of personal data across national boundaries in order to sustain international trade, freedom of speech, and intergovernmental cooperation.The latter worries arise because many national data protection laws, mostly in Europe, have long imposed restrictions on data flow to countries that do not provide comparable levels of data protection to the "exporting" jurisdiction. Although the functional influence of such rules on actual transborder data flow has been minimal, their potential impact has caused considerable concern, particularly among business interests. The A.P.E.C. Guidelines, the O.E.C.D. Guidelines, and the O.E.C.D. Guidelines all express concern about minimizing this effect in order to protect trade.[175]

---

government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation. 24. S93-S100. 10.1016/j.diin.2018.01.012.

[173]Bennett, C. J. (2011). Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies. *Journal of Comparative Policy Analysis,13*(2), 125–141.

[174]Credit China. (2018). *E-Commerce Integrity Convention*. *Credit China Shandong Qingdao Website*, 12 June 2018

[175]Custers, B., et al. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law and Security Review,34*(2), 234–243.

Privacy Framework and E.U. Directive. The latter goes the furthest in securing regional transborder data flow by prohibiting E.U. member states from instituting privacy-related restrictions on data transfer to other member states (see Article 1(2)). This ban stems from the need to expedite the completion of the EU's internal economy. Around the same time, however, the Directive goes the furthest of the foreign instruments in limiting transborder data exchange, by its competent restriction of data transmission to non-E.U. states that refuse to have "adequate" standards of data security (Article 25).

Despite their harmonising objectives, the international instruments tend to leave countries a significant degree of leeway in development of their respective data protection regimes. This is particularly true of "soft law" instruments. The legally binding instruments, on the other hand, provide for a great deal of national versatility. The C.o.E. Convention isn't meant to be self-executing, and it allows for major exceptions.Although the E.U. Directive has more prescriptive "bite" than its predecessors, it is only intended to facilitate "approximation" rather than total uniformity of national rules (see particularly recital 9 in its preamble). As a result, it gives EU member states a lot of space to maneuver.

About forty countries have passed data security legislation, and the number is increasingly increasing. The majority of these nations are European. Indeed, at both the national and regional levels, Europe has the oldest, most detailed, and bureaucratically burdensome data security regulations. Furthermore, as previously said, Europe serves as a springboard for the most aggressive and comprehensive foreign projects in the region, owing to its supranational institutions.[176]

The following are common points of departure for national data security regimes in Europe:

- coverage in both the public and private sectors;
- coverage in both automated and manual systems for processing personal data, largely regardless of how the data was structured;
- application of broad definitions of "personal data;"
- application of extensive sets of procedural principles, some of which are seldom seen in other data protection regimes;
- more stringent regulation of such types of personal data
- restrictions on transborder flow of personal data;
- establishment of independent data protection agencies with broad discretionary powers to oversee implementation and creation of data protection rules;
- channeling of privacy complaints to these agencies instead of courts;
- extensive subjection of data processing to notification and/or licensing requirements administered by the data protection agencies.

[176]Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law and Security Review,34*(3), 477–495.

- little use of industry-developed codes of practice.[177]

While the bulk of these characteristics are typical for national data protection regimes in Europe, each country there has its own unique mix of rules; concomitantly, a good deal of variation exists in the degree to which each country shares the above-listed traits. For example, the Netherlands has already used industry-based codes of conduct to a large extent, and the E.U. Directive promotes wider use of such codes (see Article 27). Furthermore, each country's data security regimes are far from uniform.

For example, Swedish law initially worked with reasonably stringent licensing and notice provisions; now it has dispensed completely with a licensing system, cut down drastically on notification requirements and implemented "light-touch", misuse-oriented regulation for the production of unstructured electronic data. There has been movement too at a broader European level. For instance, while many early European data protection regimes relied heavily on paternalistic control mechanisms (i.e., control exercised by government bodies (primarily data protection agencies) on behalf and supposedly in the best interests of citizens (data subjects)), they now show greater readiness to rely more on participatory control (i.e., control exercised by citizens themselves), supplemented by greater readiness to embrace market mechanisms for regulation of data processing. This notwithstanding, European jurisdictions (in contrast to, say, the U.S.A.) generally still maintain a relatively non-negotiable legislative baseline for the private sector.[178]

Across the Atlantic, Canada and Argentina come closest to embracing the European approach. Canada has federal legislation in place aimed at ensuring comprehensive protection of personal data in relation to both the public and private sectors. All Canadian Provinces and Territories have also enacted data protection legislation in relation to provincial and territorial government agencies; the legislation of several provinces also covers the private sector. Data protection agencies exist at both federal and provincial levels. The E.U. Commission (hereinafter "European Commission") has formally ruled that, in general, Canada offers "adequate" protection for personal data pursuant to Article 25 of the E.U. Directive. As for Argentina, it enacted legislation in 2000 modelled on the E.U. Directive and equivalent Spanish legislation, and formally based on the right of habeas data provided in its Constitution (Article 43). Like with Canada, the European Commission has formally ruled that Argentina satisfies the E.U. Directive's adequacy criterion.[179]

Mexico might well be joining this "adequacy" club in the not too distant future as it has fairly comprehensive data protection legislation in place for the public sector and similar legislation for the private sector was recently passed by the Mexican Senate. It has also established a data protection authority (Federal Institute of Access to Information and Data Protection).

By contrast, European-style data protection authorities do not exist in the U.S.A. and its legal regime for data protection is relatively atomised. While there is quite

[177] European Commission. (2018). *The GDPR: new opportunities, new obligations*. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf.

[178] Gao, H. (2018). EU personal data protection practices and enlightenment. *Secrecy Science and Technology,9*, 53–59

[179] Goncalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research,23*(2), 139–152.

extensive legislation dealing with federal government agencies, omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data protection in relation to the latter takes the form of ad hoc, narrowly circumscribed, sector-specific legislation, combined with recourse to litigation based on the tort of invasion of privacy and/or breach of trade practices legislation. At the same time, though, a "safe harbour" agreement has been concluded between the U.S.A. and E.U. allowing for the flow of personal data from the E.U. to U.S.-based companies that voluntarily agree to abide by a set of "fair information" principles based loosely on the E.U. Directive. Despite slow corporate take-up in its early days, the scheme now has over 2000 corporations (including major businesses) formally certifying adherence to it. Although the European Commission has determined that the scheme satisfies the Directive's adequacy test in Article 25, considerable evidence has since accrued to indicate significant shortcomings in the scheme's effectiveness in delivering real privacy protection.

In the Asia-Pacific region, there exist a handful of relatively comprehensive legislative regimes on data protection – most notably those in Australia, New Zealand, Hong Kong, South Korea and Japan. The bulk of these jurisdictions – but not Japan – have also established data protection authorities. New Zealand has been the fastest and most ambitious of these jurisdictions in the data protection field; it was the first to enact data protection legislation applying across the public and private sectors. Australian, South Korean and Japanese legislation in the field was initially limited largely to regulating the dataprocessing activities of government agencies, but has since been extended to cover the private sector as well.However, some of these expansions do leave significant coverage holes in the private sector. Some elements of the legislation in question deviate from the European Union paradigm as well (s). The European Commission is yet to officially recognize any of the countries involved as providing appropriate security under the EU Directive.

Data protection regimes in other Asia-Pacific jurisdictions tend to be even more patchy in coverage. Malaysia, for instance, has recently introduced data protection legislation to cover parts of the private sector but lacks equivalent legislation for personal information processed by government agencies.[180]Singapore has so far decided to establish a data protection regime based largely on voluntary, self-regulatory schemes that are linked with its national trust mark programme. As for the People's Republic of China, there exists formal constitutional protection for privacy-related interests, augmented by a patchwork of sectoral laws on point. There have been signals over recent years that the country is on the verge of introducing relatively comprehensive data protection legislation, but no such law has yet been enacted. Much the same can be said of India. Although the country has previously been reported to be considering enactment of a data protection law modelled on the E.U. Directive (largely due to fear that its burgeoning outsourcing industry will flounder without such legislation in place),no such law has yet emerged. Legal regimes for data protection are least developed in Middle Eastern and African countries taken as a whole.

As noted above, the African Charter on Human and People's Rights of 1981 omits mentioning a right to privacy in its catalogue of basic human rights. Moreover, the bulk of African countries have yet to enact European-style data protection laws. Nonetheless, some such laws have recently emerged, chiefly in francophone African

[180]Helsper, E. J., &Reisdorf, B. C. (2017). The emergence of a "digital underclass" in Great Britain and Sweden: Changing reasons for digital exclusion. *New Media and Society,19*(8), 1253–1270.

states, such as Burkina Faso, Tunisia, Morocco and Mauritius. This development partly reflects efforts by the French data protection authority (Commission de l'Informatique et des Libertés (CNIL)) to cultivate data protection in former French colonies, but it also reflects economic concerns, particularly the desire by some of these countries to safeguard their outsourcing industry (the case with, e.g., Tunisia and Morocco). Of the non-francophone states, the Republic of South Africa has come furthest along the path to establishing a comprehensive legal regime on data protection. Section 14 of its Bill of Rights, found in Chapter 2 of its 1996 Constitution, makes explicit provision for a right to privacy. A general right to access to records maintained in both the public and private sectors is also included (in section 32). In 2002, law focused on the above right was passed, and progress is currently underway on a bill for separate data privacy legislation.

As for the Middle East, Israel has long had a legislative regime for privacy and data protection in place and has been recently assessed by the E.U.'s Article 29 Working Party as passing the E.U. adequacy test. And, as noted above, Dubai passed data protection legislation in 2007 – the first (and hitherto only) Arab state to do so. That legislation, however, applies only to the Dubai International Financial Centre, not to data-processing activities in the rest of Dubai.

4.4RELATIVE IMPACT OF REGULATORY REGIMES

Comparative analysis of the effects of the different regulatory systems discussed above is both difficult and fraught with pitfalls. The task's complexity stems in part from the many facets of impact measurement: impact must be assessed in terms of economy (i.e., the cost of setting up the regime), efficiency (i.e., the cost of the regime compared to its practical results), effectiveness (i.e., the extent to which the regime's practical results achieve its ultimate goals), and equity (i.e., the extent to which the regime's practical results achieve its ultimate goals) (i.e., the extent to which the regime extends protection equitably across social groups).[181]The fact that each country's data security regime consists of more than just formal legislative regulations further complicates matters. Although the latter, along with structured oversight processes, are essential components of a data protection policy, they are augmented by a complex number of other instruments and structures – such as database systems, business codes, and guidelines – that affect the operational effect of the legal rules at the same time. The functioning of a data protection regime (including, of course, the extent to which "law in books" equates with "law in practice")[182] will also be shaped by a myriad of relatively informal customs and attitudes which prevail in the country concerned – e.g., the degree to which the country's administrative and corporate cultures are imbued with reverence for authority or values of "equal knowledge." Many of these variables, it goes without saying, are quickly misunderstood or misinterpreted. Because of their nature, it cannot be concluded that a data protection body with strong institutional powers would often be more effective in achieving its goals than one with less formal powers.Another complicating factor is that certain data protection authorities'

[181]Qin, S. (2018). *Research on the protection of personal information in the context of e-commerce in China*. Hebei: Hebei Normal University.

[182]Ren, Y., Cheng, F., Peng, Z., Huang, X., & Song, W. (2011). A privacy policy conflict detection method for multi-owner privacy data protection. *Electronic Commerce Research,11*(1), 103–121.

enforcement approaches may obscure their constructive accomplishments. Rather than openly reaching out with threats of economic penalties, agencies frequently tend to settle controversy in a comparatively discreet manner requiring "backroom" negotiation. Furthermore, authorities are often almost as concerned, if not more so, with preventing an unrealized opportunity for privacy-invading activity as they are with offering a solution after such activity happens. Measuring the effect of anticipatory control is more complex than measuring the impact of reactive, ex post facto control.[183]

Finally, some fair criticisms of data security regimes in general should be considered. One line of critique is that the regimes have yet to cultivate an institutional emphasis, as shown by the lack of direct regulatory support for privacy-enhancing technology. Another point of contention is the judiciary's marginalization; in many nations, courts have played little, if any, active role in creating and implementing data privacy regulations.This condition not only results in a lack of definitive advice on how to view the applicable laws correctly, but it also leads to data protection's marginalization as a legal area.

4.5 LET'S SUM UP

As for harmonisation efforts at the regional level, the track record of A.P.E.C. is yet to be firmly established. Within the E.U. – home to the hitherto most ambitious efforts – harmonisation remains incomplete. A large question mark hangs also over the ability of the E.U. to bring the data protection regimes of non-European states in line with its preferred model. This is presently due not so much to the recent emergence of A.P.E.C. as a potential competitor in the role of data protection "superpower"; there is as yet little evidence to show that A.P.E.C. can offer close competition in this regard. Rather, the weak implementation of Articles 25–26 in the E.U. Directive is more immediately critical. How those rules are implemented, constitutes an important litmus test for the Directive's international credibility and success. Significant problems with E.U. member states' implementation of those rules are noted above. The European Commission's tardiness in issuing adequacy findings exacerbates these problems. In the space of over a decade, only a handful of countries have so far received an adequacy stamp – and most of them are scarcely major powers in a global context.This tardiness is not surprising: proper adequacy assessments are inevitably intricate, time-consuming tasks. Unfortunately for the Directive, its regime for transborder data flow to third countries is caught between "a rock and a hard place": if properly implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large-scale avoidance of its proper implementation due precisely to fears of such procedures.

4.6FURTHER READING

- Wunsch-Vincent, S., WTO, E-Commerce, and Information Technologies: From the Uruguay Round through the Doha Development Agenda, Report for U.N. I.C.T. Task Force (Markle Foundation 2005).

[183]Ryz, L., &Grest, L. (2016). A new era in data protection. *Computer Fraud and Security,2016*(3), 18–20.

- Bygrave, Where have all the judges gone? Reflections on judicial involvement in developing data protection law, in Wahlgren, P. (ed.), IT ochjuristutbildning. Nordisk årsbokirättsinformatik 2000, Jure AB, Stockholm 2001, p. 113– 125;
- European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Brussels, 15th May 2003,.

4.7CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **What are the common points of departure for national data protection regimes in Europe?**

   The common points of departure include coverage of both public and private sectors; coverage of both automated and manual systems for processing personal data largely irrespective of how the data are structured; application of broad definitions of “personal data and many more.

4.8 ACTIVITY

Elucidate the national data protection regimes in Europe. (1000-1500 words)

યુનિવર્સિટી ગીત

સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ
સ્વાધ્યાયઃ પરમં તપઃ

શિક્ષણ, સંસ્કૃતિ, સદ્‌ભાવ, દિવ્યબોધનું ધામ
ડૉ. બાબાસાહેબ આંબેડકર ઓપન યુનિવર્સિટી નામ;
સૌને સૌની પાંખ મળે, ને સૌને સૌનું આભ,
દશે દિશામાં સ્મિત વહે હો દશે દિશે શુભ-લાભ.

અભણ રહી અજ્ઞાનના શાને, અંધકારને પીવો ?
કહે બુદ્ધ આંબેડકર કહે, તું થા તારો દીવો;
શારદીય અજવાળા પહોંચ્યાં ગુર્જર ગામે ગામ
ધ્રુવ તારકની જેમ ઝળહળે એકલવ્યની શાન.

સરસ્વતીના મયૂર તમારે ફળિયે આવી ગહેકે
અંધકારને હડસેલીને ઉજાસના ફૂલ મહેંકે;
બંધન નહીં કો સ્થાન સમયના જવું ન ઘરથી દૂર
ઘર આવી મા હરે શારદા દૈન્ય તિમિરના પૂર.

સંસ્કારોની સુગંધ મહેંકે, મન મંદિરને ધામે
સુખની ટપાલ પહોંચે સૌને પોતાને સરનામે;
સમાજ કેરે દરિયે હાંકી શિક્ષણ કેરું વહાણ,
આવો કરીયે આપણ સૌ
ભવ્ય રાષ્ટ્ર નિર્માણ...
દિવ્ય રાષ્ટ્ર નિર્માણ...
ભવ્ય રાષ્ટ્ર નિર્માણ

DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY
(Established by Government of Gujarat)
'Jyotirmay' Parisar,
Sarkhej-Gandhinagar Highway, Chharodi, Ahmedabad-382 481
Website : www.baou.edu.in