Directorate of Distance Education
Centre for Distance and Online Education (CDOE)
NALSAR University of Law, Hyderabad

Reading Material

ONE YEAR ADVANCED DIPLOMA IN CYBER LAWS

1.4 CYBER SECURITY & CYBER CRIMES

By:

Dr. K. V. K. Santhy
Associate Professor
NALSAR University of Law, Hyderabad
&
Mr. Na. Vijayashankar

Privacy and Data Protection Consultant

First Edition 2019
Re-Print 2021
(For private circulation only)

Contents

Page No.

CHAPTER I: INTRODUCTION TO CYBER CRIMES

Introduction:

The term 'cyber law' in general refers to all the legal and regulatory aspects of Internet. It means that anything concerned with, related to, or emanating from any legal aspects or issues concerning any activity of netizens and others in cyberspace comes within the ambit of cyber law. More specifically, cyber law can be defined as a law governing the use of computer and the Internet. Namely, it focuses on a combination of state and federal statutory, decisional and administrative laws arising out of the use of Internet.

The IT revolution resulted in a phenomenal increase in the number of cyberspace[1] users all over the world. The birth of the Internet resulted in networking which helped millions of users to connect online, thus facilitating the sharing of information. In India also, there was an overwhelming increase in the number of internet-users. *Forrester Research*, a technology and market research Firm reported that the number of internet-users worldwide would touch the 2.2 billion mark by 2013 and that India would have the third highest number of internet-users at the same time.[2] The government framed and announced Internet policy document in 1997[3] to promote and encourage internet-users in India.[4] With economic activities like buying, selling, advertising, etcetera taking place online, the Internet indeed proved to be a boon for many. Little did anyone suspect that the uncontrolled manner in which online activities were carried on would give way to another category of computer related crimes. Cyber crime is a new type of criminal activity that started raising its ugly head in the early 1990s, as the Internet emerged as a virtual place for the users worldwide to meet and share various forms of Information. This development also paralleled with the entry of criminals to gain access to sensitive information if they have the necessary knowhow. Thus the Cyber space became vulnerable from the economic and social perspectives- driving companies and individuals to take costly steps to ensure their safety and exposure from those deviant acts in the cyber space.

---

1 William Gibson coined the term cyberspace in his science fiction novel *Neuromancer* written in early 1980s. The plot was largely set in a setting that had no physical existence. The plot involved a hacker employed by an anonymous employer to hack. Cyberspace was a conceptual hallucination that felt and looked like a physical space, but was actually computer-generated. In this setting, people, connected to network, carried out business transactions, worked, played and broke the law.
E.A. Cavazos and Govino Morin, *Cyberspace and the Law: Your Rights and Duties in the online world* (1994), p. 1

2 The Times of India, *India to have 3rd largest number of internet users by 2013*, July 26, 2009 *available at* http://articles.timesofindia.indiatimes.com/2009-07-26/india-business/28171189_1_internet-users-online-population-asian-markets (last visited July 11, 2011)

3 Internet Policy of Government of India-1997

4 *Bharat's Hand Book of Cyber and e-commerce Laws,* Edited and compiled by P.M. Bakshi and R.K. Suri,, Bharat Publishing House, New Delhi, 2002, p. 12

1.1 Cyber Law and Cyber Crime:

One of the early cyber crime, which had come to the public notice is the fraud relating to fund transfer online to the tune of USD 10 Million from Citibank. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack compromising the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers to commit the cyber crime. He was finally arrested on Heathrow airport on his way to Switzerland.

Cyber Crimes increased by 22.7% in 2007 as compared to 2006 (from 453 in 2006 to 556 in 2007), Cyber Forgery 64.0% (217 out of total 339) and Cyber Fraud 21.5% (73 out of 339) were the main cases under IPC category for Cyber Crimes. In this 63.05% of the offenders under IT Act were in the age group 18-30 years (97 out of 154) and 55.2% of the offenders under IPC Sections were in the age group 30-45 years (237 out of 429) according to the latest data available with the National Crime Records Bureau of the Ministry of Home of Government of India.

The Information Technology Bill (1999) has defined the cybercrimes as:

'*Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when computer source code is required to be kept or maintained by law for the time being in force* [shall be punishable with a fine which may extend up to rupees two lakhs or with imprisonment up to three years, or with both].'

1.2 Classification of Cyber Crimes:

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, and theft of intellectual properly. Cyber crime in the context of national security may involve hacking, traditional espionage, or information warfare and related activities.

Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

Broadly there are two classes of cyber crimes:

A. ***Computer Assisted Cyber Crimes: computer is instrumental in committing the crime*.**

- Selling nonexistent, defective, substandard or counterfeit goods, theft of credit card, bank fraud, fake stock shares, intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books
- Selling obscene and prohibited sexual representations.

B. Computer Oriented Cyber Crimes: Computer is the target of the crime

- Malicious Software: viruses, Trojans (which corrupt server)
- Cyber terrorism:
- Child pornography
- Violent and extreme pornography
- Internet inspired homicides and suicides

❖ *Worm: Self-replicating programmes, spread autonomously without a carrier.*

Ex. Via mail, scanning remote systems

❖ *Trojan: installed during downloading some programme as a back ground activity causing irreparable damage*

❖ *Spyware: parasitic software-invades privacy-divulging details- through tracking cookies.*

Even though our basic understanding about cyber crime is that computer is necessary as one of the components of the offence, it is also interpreted that a crime committed by using any digital device is covered under the ambit of cyber crime. For example: Casio digital diary, Mobiles, Calculators, Pen drives, CDs.

1.3 Cyber Security:

Cyberspace is as vulnerable as much as it is a vital infrastructure. The threat is real. US President Obama recently declared that "cyber threat is one of the most serious economic and national security

challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security." The same is true for other nations as well. Private and public cyber infrastructure in the United States falls under nearly constant attack, often from shadowy sources connected to terrorist groups, organized crime syndicates, or foreign governments.[5]

These attacks bear the potential to disrupt e-mail and other online communications networks, but also the national energy grid, military-defense ground and satellite facilities, transportation systems, financial markets, and other essential facilities. In short, a substantial cyber-attack could take down the nation's entire security and economic infrastructure. Cyber is the new domain of international espionage, sabotage, and war. China, Russia, the United Kingdom, and the United States employ extensive cyber spying networks." A coordinated series of denial-of service and other attacks could cripple a state's political and communications systems, as happened during "Web War 1" between Russia and Estonia in 2007[6] as computer networks collapsed, factories and chemical plants exploded, satellites spin out of control and the financial and power grids failed." In June 2010, for example, a computer worm called "Stuxnet" was discovered in Iran. At first inspection, it appeared to be a routine bit of malware. Closer analysis, however, revealed that Stuxnet was carefully designed to disrupt the sort of systems that help control equipment at nuclear power plants. Stuxnet's subtlety and sophistication suggested to most experts that it was engineered not by rogue hackers, but rather by an entity with the resources of a nation-state, and that it was specifically targeted to damage Iran's nuclear capabilities. Many Analysts suspected that it was coordinated and launched by Israel or the United States.[7]

Recent evidence suggests that Stuxnet successfully curtailed Iran's production of refined uranium. The Stuxnet attack appears to have bled into "real" space: the Iranian scientist chiefly responsible for eradicating Stuxnet from Iran's nuclear plants was killed on November 29, 2010, by assassins on motorbikes, who threw a bomb when he was driving his car.

Trojan horse- Program that performs some ostensibly useful function but contains, lurking within its code, a damaging instruction set. Often, that instruction set will enable a remote user to assume control of a system, or will secretly introduce unwanted software into a system. Indeed, Trojan horses are probably the most common way in which viruses are introduced into computer systems. While technologically complex, and once the sole province of sophisticated users, Trojan horses now are readily available from websites catering to would-be hackers. For example, the "Cult of the Dead Cow," a group

---

[5] CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1 (2008) [hereinafter CSIS REPORT], available at http://csis.org/files/media/csis/pubs/081208_securing cyberspace 44.pdf)

[6] The Threat from the Internet: Cyberiar, ECONOMIST, July 3, 2010, at 50, available at http://www.economist.com/node/16481504?storyid=16481504&CFID=158391401&CFTOKEN=341 82131.

[7] (Kim Zetter, Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage, WIRED THREAT LEVEL (Nov. 15, 2010, 4:00 PM), http://www.wired.com/threatlevel/2010/11 /stuxnet-clues.)

of cyber-anarchists devoted to keeping the web free, created a program known as "Black Orifice 2000" that when downloaded from a user's e-mail, enables a remote user to take advantage of security problems with Windows and allows a remote user to control the target's computer.

Password sniffers **-** Password sniffers are programs that monitor and record the names and password of Internet users as they log on to the network. The programs work by collecting bytes of the computer that is being monitored by the installer of the sniffer. When a network user types in a user name and a password, the sniffer collects the information and passes it on to the installer. With the use of this information the installer logs on to the system, has access to restricted documents and can manipulate information held therein.[8]

A virus is a program that modifies other computer programs. The modifications ensure that the infected program replicates the virus. In other words, the original program (the analogue to a healthy cell) is changed by the virus so that the virus can multiply. Once infected, the program secretly requests the computer's operating system to add a copy of the virus code to the target program.

Once that computer is connected to another computer, either through the Internet, direct computer connection, or even through a common floppy disk, the virus may spread beyond the original host computer. A virus is not inherently harmful-its harmfulness will depend on the additional codes placed into the virus besides the code for self-replication. Some viruses, however, have caused enormous damage.

The Melissa virus **-** Melissa infected its first victim when a reader of the pornographic alt.sex newsgroup caught it. Within days of this initial contact, Melissa infected more than one hundred Fortune 1000 companies. The virus operated by e-mailing a list of eighty pornographic web sites to fifty e-mail addresses in the electronic address book of the infected system. Id. The fifty recipients received e-mails with the subject line "Important Message From..." and the virus automatically filled in the initial user's name-so that it appeared that the recipient was receiving a message from his or her friend, rather than from the Melissa culprit.

Worms **-** A worm is a stand-alone program that replicates itself. Both worms and viruses self-replicate. The distinction is that while a virus requires human action, from downloading a specific file to placing an infected disk in a computer, a worm uses a computer network to duplicate itself and does not require human activity for transmission. For example ‘I love you virus’ bred on a hosts computer and it reproduced over a network. Most companies, including AT&T Corp., Ford Motor Co., and Merrill Lynch & Co., shut down their e-mail systems to prevent a spread of the attack, resulting in lost time and

[8] (66 J. Crim. L. 269 2002)

productivity. Government agencies were also affected, including the Pentagon, the CIA, NASA, the Swiss Government, Danish Parliament, and the British House of Commons.

Investigators traced the 'I Love You bug' to several computer students in the Philippines, but the case was ultimately dropped because the Philippines had no applicable law against viruses or hacking.

Some Illustrations :

E -mail Cheating -Mr. Vijay Ninwane works at Abu Dhabi. He was sent a mail by one X saying that she is interested in him. Both of them exchanged nude photos, erotic stories etc. "x" introduced her friends y1, y2, y3, y4. Vijay could not meet x as promised as a result of which she committed suicide. Then Vijay received mail from WWW.KOLKATTA_POLICE.COM, WWW.CBI_HQ.COM alleging that he is responsible for her death and he would be prosecuted for the same. Vijay contacted Y1 for help. Y1 coaxed Vijay to have a lawyer and she will help him to get a lawyer. Accordingly Y1 fixed Mr. Pranab Mitra of Mitra & Mitra associates and made him believe that they are the leading lawyers. Vijay paid total Rs.70 lakhs (Rs.1.19 crore as per investigating officer). During the investigation it was revealed there is no girl by name X and Y1 and others are also fictitious persons created by one single man named Mr. Pranab Mitra, General Manager of the Firm.[9]

Cyber Murder **-** A patient was admitted in New York Hospital. The entire system was computerized in the hospital. One cracker entered the system and modified the data relating to amount of insulin to be injected to a patient as a result of which, 60mg was modified into 260mg. Nurse injected the same amount of insulin to the patient and he died.

PHISHING **-** Using spoof e-mails or directing people to fake web sites to fool them into divulging personal financial details so criminals can access their accounts.

PHARMING **-** Technically more sophisticated and it means exploitation of vulnerability in the DNS server software. Approximately 7.9 million phishing attacks are made per day on pentagon. There is a tremendous increase of 39% over first half of 2005.

1.4 Distinction between cybercrime and conventional crime:

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

[9] P Krishna Sastry, Forensic Expert, Questioned Documents, Hyderabad.

The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Indian Penal Code to mean as an act or omission made punishable by any law for the time being in force.

Sir William Blackstone defines crime as a Act committed or omitted in violation of a public law forbidding or commanding it.

Sir C.K. Allen (The Nature of a crime) proposes that “Crime is crime because it consists in wrong doing which directly and in serious degree threatens the security or well-being of the society, and it is not safe to leave it redressable only by compensation of the parties injured”.

Wolfenden Committee (England) tried to explain crime as “The function of criminal law is to preserve public order and decency, to protect the citizen from what is offensive or injurious, and to provide sufficient safeguards against exploitation and corruption of others, particularly those who are especially vulnerable. It is not a function of the law to intervene in the private lives of citizens or to seek to enforce any particular pattern of behaviour, further than is necessary to carry out the purposes which we have outlined”.

The general laws in the area of criminal law commonly referred are the Indian Penal Code, 1860 (“IPC”), which is the general penal law of India and the Indian Evidence Act, 1872 (“Evidence Act”), the general law pertaining to admissibility of evidence in civil and criminal trials. The manner in which trial of criminal cases are to be conducted is dealt with under the Criminal Procedure Code, 1973 (“Cr. P. C”).

To understand ‘cyber crimes’ and its ramifications in terms of the damage, the challenge to prosecution, the loopholes of the existing criminal justice system, the powers of regulation and its boundaries, it is essential to have look at the concept of ‘crime’ itself.

In every organized society, certain acts and omissions are forbidden on pain of punishment, which may even extend to the forfeiture itself. What acts or omissions should be singled out for punishment or be branded as crimes has always depended on the force, vigour and movement of public opinion from time to time to and country to country and even in the same country from decade to decade.

Dowry was considered as a ‘social status’ at a particular period, which today is a crime. Untouchability was an accepted social norm of a particular period in society in tune with caste hierarchy and today it is a crime under the constitution. Thus very many acts are crime today, which are not once, and some acts like homosexuality or lesbianism, which is a crime today, could change tomorrow. In essence the ‘concept of crime’ is static in some aspects such as stealing, fraud, causing injury, murder etc. and changing in certain aspects of social norms and relationship.

Similarly ‘crime’ in a society is not a crime in another society. What could be considered as ‘obscenity’ in India could be viewed differently in Sweden. For example watching pornography is not a crime in England, whereas in India public watching, transmission of porn material is an offence.

As it is very difficult to explain and define a ‘crime’ , we can describe it and may state that in a crime we find at least three attributes mainly first that it is a harm brought about by some anti social act of a human being, which sovereign power wants to prevent, secondly the preventive measures taken by the state appear in the form of threat of a sanction or punishment and thirdly the legal proceedings wherein the guilt or otherwise of the accused is determined are a special kind of proceedings governed by special rules of evidence.

A crime consists of following components. a) Human being b) ***Mens Rea***- the mental state of the person accused of a criminal act or guilty mind c) ***Actus Reus***- committing an act or omission of an act when it is warranted resulting in a criminal act d) harm to body mind or reputation.

Yet another very important aspect of crime is that 1. A particular act or omission shall be recognized by a law as an offence and 2. There shall be a punishment prescribed for the offence recognized.

The legal debate surrounding ‘cyber crimes’ is twofold. The first challenge is to define what constitutes ‘cyber crimes’ as opposed to ‘physical crimes’ and the second challenge is that of the application of traditional criminal law and criminal justice administration on the ‘cyber crimes’. In the first debate on what constitutes ‘cyber crimes’ there is some consensus. Legal analysts have a consensus that ‘cyber crimes’ are those crimes perpetuated using computers and computer networks through the medium of Internet to perpetuate various cyber crimes. Such crimes are committed:

It is on the second aspect of analysis, whether ‘cyber crimes’ need a different interpretation of the criminal law concepts, there are divergent views. Whether there should be a separate ‘cyber crime laws’ or whether traditional criminal law is enough? How to assess and compute the damages in ‘cyber crimes’ using the traditional analysis of criminal law used in the concept of ‘physical crime’ and related issues. Additionally the nature of ‘cyber crimes’ by virtue of the internet is a crime which poses challenge to international conduct and hence the need for an international dimension of ‘cyber crimes’ which is considered as the ‘international warfare of Information technology’.

On the regulation of the ‘cyber crimes’ again there is a wide debate on how far one can regulate and what type of regulations should be in place. There could be consensus on the regulation of ‘cyber crimes’ such as hacking, fraud, obscenity and related crimes, where as the human right activists, votaries

of privacy and other activists accuse violations of the authority on the name of security and cyber crime where their civil rights are curbed, activities monitored and privacy intruded.

The term ‘cyber crime’ is a misnomer. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. However, there are certain differences between the two. It would be relevant to points out these similarities and differences between the two.

1.5 Requirement of guilty mind for cyber crimes:

To be guilty of cybercrime in India, a person must act voluntarily and willfully. For example, a person who deliberately sends Viruses online is guilty of cybercrime; a person who forwards an e-mail without realizing it contains a virus or spreads a virus when her account is hacked is not guilty.

Sec 65, 66 and 67 of IT Act mandates that offences recognised under these provisions shall be committed by the accused intentionally. Intention, knowledge, fraudulent intention, connotes various forms of guilty mind. The following is a brief explanation of some phrases used in IT Act connoting guilty mind.

Intention:

1. Design of doing an act

2. Purpose/ design with which an act is done. It is also the **expectation** that certain consequences will follow from the **conduct** of a person. Conduct is the proof of intention.

Noted Jurist Salmond says that every wrongful act may raise two distinct questions with respect to the intention of the doer. How did he do the act? Why did he do it? First is an inquiry into intention. Second is concern with his ulterior motive.

Knowledge and belief:

Knowledge is the awareness of facts**.** If an accused knows the consequences or have the awareness of the facts it is deemed that he has guilty mind**.**

Dishonest Intention:

Sec 24 of IPC defines "Dishonestly" as,

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Sec 25 of IPC defines "Fraudulently" as,

A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

The IT Act, Sec 66B uses the word 'dishonest intention' which is not defined in the Act, then one can refer to IPC which is a general legislation in the area of criminal law.

Law of Attempt:

Person commits offence of attempt to commit an offence when he/she

1. Intends to commit that particular offence
2. He having made preparation with an intention to commit an offence, does an act towards commission
3. Such an act need not be the penultimate act towards committing that offence, but should be an act during the course of committing that offence.
4. Such act must be proximate to offence.

Measure of proximity is not in relation to time and action, but in relation to intention

There are five kinds of punishments recognized by IPC, 1860 - Death, Imprisonment for Life, Imprisonment Rigorous and simple, Forfeiture of Property and Fine.

Information Technology Act, 2000 for cyber crimes prescribes two kinds of punishments i.e. imprisonment and fine.

How to judge whether particular incident is a crime?

Example 1: Mr. Ram bolts the door of a house belonging to X from outside and sets fire, resulting in death of four inhabitants. If we analyse the case, first point is Ram is a human being had it been a

monkey not liable, second he had an intention to burn the house and kill the inhabitants which is clear from his conduct of bolting door from outside, three he committed the forbidden act of burning and fourth there is harm which is death of four people. Hence it is a crime of Murder punishable under Sec 300 of IPC with either Life imprisonment or death.

Example 2: A fired a shot at a bush in a thick forest thinking there is a tiger behind it, but there is a person who died of the shot. The question is whether he is liable. He is not liable because he doesn't have the required guilty mind; his intention was to kill a tiger.

Thus the penal provisions will act upon the application of the above basic elements in any crime in the physical world. The basics of such is in the first place, any legal system should first define certain acts as criminal which is harmful to the society and there upon the actions that are considered as crime will be subject to the scrutiny of the above elements of intention, conduct, circumstance and prohibited act to evoke the required penal provisions. The fundamental principle is that a conviction is possible only if there is a concrete proof beyond reasonable doubt that the act of a person is prohibited by the criminal law and such an act is also committed with an intention of causing the same.

1. 6 CRIME IN CONTEXT OF CYBER CRIMES:

The cyber world is defined as a virtual world, which is different from that of the physical world. The cyber world though a virtual world is a reality, which interconnects, people, organizations, Governments. It transacts information at the basic level but also conducts the business of governments and private enterprises in a manner where no other technology could dream of. The cyber space is also a space where various types of crimes are perpetuated and the magnitude of such crimes could be unimaginable due its speed, anonymity and destruction has been amply recorded. The moot point is whether the same principles of criminal law can be applied to the 'cyber world crimes' as applied to the 'world of physical crimes'. The answer is divided.

One school of thought advocate that it is possible to interpret the crimes perpetuated in the cyber world to that of the physical world and hence could apply the same principles to regulate them. To substantiate the following arguments are held forth:

1. 'Cyber Crimes' are nothing but crimes of the physical world perpetuated in the world of computers and hence there is no difference in defining a crime in the cyber world and the physical world

2. As in the physical world the cyber world crimes are perpetuated by individuals or groups, where the medium is the only difference.

3. As the traditional principles of criminal law have tackled various technologies used in the past it is capable of analyzing and interpreting the new technology as well.

4. The cyber crimes in fact are lesser in scope than the physical crime like fraud, intrusion of privacy, data theft, damage to computers, cheating consumers etc. where as physical injury or other crimes like rape, grievous hurt or bigamy cannot be perpetuated through the cyber crimes.

5. The technological advancement of the information technology itself is a deterrent and a tool in tracking and convicting the crimes.

On the other hand there are advocates who say that 'cyber crimes' cannot be tackled with the conventional principles of 'cyber crimes' and thus need special laws to regulate them and they put forth the following arguments:

1. Cyber Crime is a crime, which has a potential and uncontrollable damage and needs stricter regulations. A virus introduced can damage millions of computers before even finding the perpetuator.
2. The cyber crime is perpetuated by anonymous person who has to be skilled in opening the password and security systems and can vanish without a trace.
3. The cyber crimes are transnational in nature, which involves complex prosecution procedures to bring the culprits to the book.
4. The Cyber crime of obscenity and pornography has a potential moral depravity on generations which could push them into the physical world of crimes
5. The National Security and security in terms of safety like Airports, Railway systems are more vulnerable and could create chaos and economic loss by cyber crimes and hence special laws to apprehend, prosecute with stiffer penalties are needed in context of cyber crimes
6. The technology is a fast changing one and hence needs a different type of enforcement system to tackle the cyber crimes unlike the physical crimes.

1.7 Punishments under IT Act:

With the debate on the above lines continuing one thing is clear that cyber crimes has the potential to damage the economic aspects of a society and a nation due to technology where speed, ease of operation, defying boundaries are strengths and weaknesses at the same time. The legislations around the world are veering around to the view that 'cyber crimes' warrant stricter penalties due to its quantum

of damage. There are also attempts to address the technology related issues by setting up of 'cyber tribunals'.

In Indian context, the IT Act of 2000 tries to address the question of 'cyber crimes' by defining what is a damage in the context of the computers and the relevant penalties as follows:

Imprisonment for a specific period of time and fine is prescribed as punishments for cyber crimes in the Act. It is not clear from provisions whether imprisonment is of rigorous or simple in nature. The fine amounts are in tune with the losses incurred in cyber world and are quite deterrent in nature. For Example Sec 66 IT imposes two lakhs of rupees as fine.

Confiscation:

Section 76 provides that Any computer, computer system, floppies, compact disks, tape drives or nay other accessories related thereto, in respect of the if which any provision of this Act, rule, orders or regulations made there under 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 there under, 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 authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Residuary Penalty:

According to Section 45, whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Non-Interference with other Punishments:

According to Section 77 of the Act, No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

CHAPTER II: LAW RELATING TO CYBER CRIME

Introduction:

This chapter is devoted to discuss the substantial law regarding cyber crimes recognized by Information and Technology Act, 2000 and the amendment Act, 2008. Chapter XI of the Act defines various cyber crimes and prescribes punishments for the same. It focuses on various offences such as Hacking, Cyber Stalking, Data Theft, and Introduction of worms and viruses, obscenity and child pornography. The genesis of every cyber is available in the general criminal law of India ie, Indian Penal Code, hence relevant provisions from the code are referred along with IT Act. The Act totally has 13 chapters and 90 sections[10]. The Act begins with preliminary and definitions and from thereon the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and since replaced by electronic signatures in the ITAA -2008) have been spelt out. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described.

2.1 Cyber Crime Jurisdiction:

Every law enacted in India is applicable to the whole of Indian Territory. Indian law is applicable to Indians who live on foreign territory as well. Sec 3 of Indian Penal Code imposes liability on a person beyond Indian Territory. They can be tried according to the Indian penal laws and could be punished. Sec 4 of IPC provides for application of Penal Code to the extra territorial offences. Information and Technology Act is applicable to all states of India including Jammu and Kashmir. However cyber crime knows no boundaries. The accused would operate from some country. The problem lies in bringing them back to India. Unless they are found on the territory of this country our penal law can't be made applicable. Sec 1 of IT Act deals with the applicability of law.

Sec 75 of IT Act deals with the issue of the applicability of the Indian Cyber Law for an offence or contravention committed outside of India. Sec 75 makes the provision of the IT Act applicable to any offence committed outside India by any person, irrespective of his nationality. This enables the law to assume jurisdiction over cyber criminals outside the territorial boundaries of India. The provision uses the phrase "involving computer" thus regardless the fact that whether the involvement of a computer, computer system, or computer network is intentional or accidental or negligent, every instance is covered by the word "involving".

[10] (the last four sections namely sections 91 to 94 in the IT A 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934).

Sec.75. Act to apply for offence or contravention committed outside India. -

(1) Subject to the provision of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting located in India.

2.2 Hacking:

Sec.65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

If the accused intentionally or knowingly, destroys, alters or conceals any computer source code, computer programme or system or network, punishment provided is three years imprisonment and fine up to two lakhs of rupees. This provision penalizes unauthorized access *perse*. The complainant need not prove that he suffered any loss or damage because of the unauthorized access. If the accused alters any information of the computer because of which the value or utility is diminished, it amount to hacking. The offence is punishable up to three years imprisonment and fine up to two lakhs of rupees.

Sec.66. Hacking with computer system.-

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Hacking[11] a common term used illegal entry into the computer or networks is actually an act of unauthorized entry. This offence is covered by two provisions 65 and 66 of IT Act.

The offence as per this section involves the following elements:[12]

1. There should be intent on the part of the accused to cause wrongful loss or damage to the public or any person.

2. There should be knowledge of an attributable to the accused that he is likely to cause wrongful loss or damage to the public or any person

3. The accused must destroy or delete or alter any information residing in a computer resource

4. The accused must diminish the value or utility of any information residing in a computer resource

5. The accused must affect any information residing in a computer resource injuriously by any means.

6. Any person who breaches a protected system leaves himself open to criminal liability under section 70 IT Act. Anyone who access or attempts to access a protected system commits an offence and can be punished with imprisonment for a term of ten years and can also be fined. (Meaning of attempt: with guilty intention when an accused moves towards committing the prohibited act, which is short of accomplishment).

7. Hacking includes the following activities as per law.
    - Unauthorized access to information systems
    - Disruption, interference
    - Introduction of malicious software
    - Downloading, extraction copying
    - Destroying altering info

---

[11] Hacker (hacking) .A hacker is someone who is able to manipulate the inner workings of computers, information, and technology. Consider Arthur C. Clark's Third Law: "Any sufficiently advanced technology is indistinguishable from magic". Since normal people have no clue as to how computers work, they often view hackers with suspicion and awe (as magicians, sorcerers, witches, and warlocks). This suspicion leads to the word "hacker" having the connotation of someone up to no good. History: The word "hacker" started out in the 14th century to mean somebody who was inexperienced or unskilled at a particular activity (such as a golf hacker).
In the 1970s, the word "hacker" was used by computer enthusiasts to refer to themselves. This reflected the way enthusiasts approach computers: they eschew formal education and play around with the computer until they can get it to work. (In much the same way, a golf hacker keeps hacking at the golf ball until they get it in the hole). Furthermore, as "experts" learn about the technology, the more they realize how much they don't know (especially about the implications of technology). When experts refer to themselves as "hackers", they are making a Socratic statement that they truly know nothing.

[12] Pavan Duggal, Cyber Crime and Jurisdiction in India, P.211, TMC ASSER PRESS.

Hackers are those who hunger for details about computer systems and use devious or even illegal means to satisfy their curiosity. By using software tools, hackers can break into computers to steal data, plant viruses or work any other mischief. Manipulation and disruption of electronic information by hackers through access to voice-mail, e-mails and long-distance telephone connections are costing companies more than $1 billion every year.' In September 1999, for example, hackers broke into and vandalized the websites of NASDAQ and the American Stock Exchange which was referred to as 'a bold electronic affront to the world's financial markets'.

The offence of hacking, if committed with an intention of committing further offences, a parallel for such offences can be drawn from the offences of theft, fraud, misappropriation, forgery, nuisance etc. If a person gains unauthorized access to the Property (website) of another, breaching confidentiality of electronic documents, the same is punishable under Section 72 of the I. T. Act punishable with an imprisonment up to 2 years or fine up to 1 lac or with both.

Hacking is gaining unauthorized access to a computer or network of computers. It can be undertaken in a variety of ways from simply exploiting inside information to brute force attacks and password interception. It is often – though not always - with malicious intent to either copy, modify or destroy data. Intentional corruption of web sites or access to services protected by conditional access without payment can be one of the aims of unauthorized access. Such an act of Hacking can also include disruption of information systems.

Various Forms of Hacking: the following are some prominent and recent forms of hacking.

Disruption of Information Systems: Different ways exist to disrupt information systems through malicious attacks. One of the best-known ways to deny or degrade the services offered by the Internet is a **"denial of service"** [13] attack (DoS). In a way this attack is similar to fax machines being flooded with long and repeated messages. Denial of service attacks attempt to overload web servers or Internet Service Providers (ISPs) with automatically generated messages. Other types of attacks can include disrupting servers operating the domain name system (DNS) and attacks directed at "routers". Attacks aimed at

[13] DoS (Denial of Service) An exploit whose purpose is to deny somebody the use of the service: namely to crash or hang a program or the entire system. Example: Some classes of DoS are: traffic flood. Overwhelms the Internet connection. Because it is the Internet connection itself that is attacked, there isn't much the victim can do to stop the attack. A firewall might block the flood from going any further, but the Internet connection in front of the firewall is still overloaded. Application floods or bombs Overwhelms a program with too many events. A firewall that allows the traffic cannot block these attacks. For example, a firewall configured to allow IRC cannot selectively block just the flood but allow all other traffic. Common services attacked this way are IRC, HTTP, and e-mail (SMTP). Remote system crash/hang, historically, there have been a lot of ways of remotely crashing machines. These attack the TCP/IP stack within the system causing it to crash or hang. This affects all software running on the system.

disrupting systems have been damaging for certain high profile web sites like portals. Some studies[14] have calculated that a recent attack caused damage worth several hundred million Euros, in addition to the intangible damage to reputation. Increasingly, companies rely on the availability of their web sites for their business and those companies, which depend on it for "just in time" supplies are particularly vulnerable.

Salami Attacks: These types of attacks are mainly seen in the financial area. This attack makes so small alterations so that it would go completely unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account. In this case, the man first created a logic bomb into the bank's system. Logic bombs are programmes that will get activated only at the occurrence of an event.

Execution of malicious software that modifies or destroys data: The most well-known type of malicious software is the virus. Infamous examples include the "I Love You", "Melissa" [15]and "Kournikova" viruses. About 11 % of European users have caught a virus on their home personal computer (PC). There are other types of malicious software. Some damage the PC itself, whereas others use the PC to attack other networked components. Some programs (often called 'logic bombs') can lie dormant until triggered by some event such as a specific date, at which point they can cause major damage by altering or deleting data. Other programs appear to be benign, but when opened release a malicious attack (often called 'Trojan Horses')[16]. Another variant is a program (often called a worm)[17]

---

[14] 1 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for a European Policy Approach" of 6.6.2001. COM (2001) 298 final.

[15] Melissa Virus/Worm- In early 1999, the Melissa virus/worm took down much of the Internet for a couple of days. Controversy: Many security technologies (anti-virus, firewalls, mobile code) are based upon the concept of querying the user with the question: There is a security issue here, are you sure you want to continue? Security professionals have long warned that just dependency is unreliable -- users have to be lucky in answering the questions right all the time, whereas the hacker needs to get lucky only a few times. In the case of the Melissa virus, every user that spread the virus was first prompted with the query: This document contains macros, do you want to run them?, and answered incorrectly.

[16] Whereas the general popular uses the word virus to refer to any malware, a Trojan is not technically a virus. Generally, Trojans do not spread to other programs or other machines.
The word can be used as a verb. To Trojan a program is to add subversive functionality to an existing program. For example, a trojaned login program might be programmed to accept a certain password for any user's account that the hacker can use to log back into the system at any time. Rootkits often contain a suite of such trojaned programs. Users can often break into a system by leaving behind trojaned command programs in directories (like their own directory or the /tmp directory). If you copy your own is program to the /tmp directory, and somebody else does a cd /tmp then an is, that user will run your program with their own privileges. This is especially dangerous against root, which is why the local directory should not be part of the search path for the root account.
A big fear is the transitive Trojan -- a Trojan horse that generates other Trojans. The best example is the Trojan described by Ken Thompson. He put a Trojan horse into the C compiler so that when the login code was compiled, it would always accept a backdoor password. A common technique to guard against that is to first recompile the compiler first. Thompson therefore trojaned the compiler so that when it recompiled itself, it would put back the Trojan. Therefore, even when you had the complete source to UNIX and compiler, you still couldn't recompile from scratch and remove the Trojan. The fear is that tool vendors might put such Trojans in their compilers, which cause products made from those compilers to have backdoors.

that does not infect other programs as a virus, but instead creates copies of it, which in turn create even more copies and eventually swamp the system.

New Virus: Mumbai cyber-crime cell recently notified that a new virus threat through an E-mail attachment called 'cabnote' which could damage and destroy the hard disk and other computer data as well. The word 'cabnote' s a disguise and it has nothing to do with Union or state cabinet notes.

Logic Bomb: A logic bomb tells a computer to execute a set of instructions at a certain time under certain specified conditions.'" Those commands could be benign (a nice message from the programmer each year on her birthday) or damaging (telling the hard disk to erase itself on May Day). A logic bomb can lie undetected in software or hardware, ready to be detonated when a series of events unfolds. A Trojan horse, by contrast, is a computer program that performs some apparently useful function, but which also contains malicious hidden code. The malicious code may introduce a virus or other computer bug or it may permit unauthorized access by an outside user.

***Interception of communications*:** Malicious interception of communications compromises the confidentiality and integrity requirements of users. It is often called "sniffing".

Distributed Denial of Service: **Distributed Denial of Service ("DDOS")** attacks overwhelm web sites and stop them from communicating with other computers. To carry out a DDOS attack, an individual obtains unauthorized access to a computer system and places software code on it that renders that system a "Master." The individual also breaks into other networks to place code that turns those systems into agents (known as "zombies" or "slaves"). Each Master can control multiple agents. In both cases, the network owners become third-party victims, for they are unaware that dangerous tools have been placed on their systems. The Masters are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents. After receiving this information, the agents make repeated requests to connect with the attack's ultimate target, typically using a fictitious or "spoofed" IP address, so that the recipient of the request cannot learn its true source. Acting in unison, the agents generate a high volume of traffic from several sources.

---

[17] Morris Worm-Unleashed on the morning of Thursday, November 3, 1988, the Morris Worm essentially crashed the Internet. In true worm fashion, it exploited bugs in several UNIX programs (send mail, finger) to break into machines. Once in a machine, it would then look for other machines and launch attacks against them. Due to a programming mistake, the Morris Worm would not recognize when it had already broken into a machine. As the worm multiplied, machines would get broken into over and over, eventually overloading the machine and taking it offline. The worm is named after its creator, Robert Tampa Morris.

Cases on Hacking:

Case-1. Varpaul Singh vs. State of Punjab[18]

The petitioner was working in the capacity of General Manager of M/s Makkar Motor Private Limited. In furtherance of the common intention of the accused, fictitious bills and entries were created. Important data was deleted from the computers. Related documents were taken away by way of committing the offence of theft. Spare parts had been sold/ embezzled. Substantial amount has been pocketed by the accused mentioned in the FIR. Allegation is also to the effect that he misused the confidence reposed in him by way of giving him access to the main frame. The password entrusted for a particular purpose was used to change the data in the computer system. Allegation is also to the effect that while more money was charged, the defects in the vehicles were not rectified. Bills for the work done were deleted from the computer main frame.

In November 2009, The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, a techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs.5, 000 under section 420 IPC (cheating) and Section 66 of IT Act (hacking). Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.

The CBI had registered a cyber-crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorized use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs.38, 248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore as also from Chennai and other cities, they said.[19]

Case-2. Hacker hacks into a financial website

Mumbai police have arrested a hacker by name Kalpesh (name change) for hacking into a financial website, although the hacker couldn't break into the main server of the financial institution, which was well secured by the financial institution. The accused person could make some addition to the home page of the financial website and has added a string of text to the news module of the home page of the website. Police were able to crack the case by following the trace left by the hacker on the web server of the financial institution. The financial institution has maintained a separate server for financial online

[18] (19.04.2010 - PHHC)

[19] Pasted from <http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy>

transactions, for which utmost security has been taken by the financial institution. The website was hosted on a different server which comparatively had lesser security.

The hacker Kalpesh (name changed) has done computer courses like CCNA, MCSE etc. But he is a computer addict. He goes to a particular website on the web, which facilitates him to see the entire directory structure of that website. Then using various techniques, such as obtaining a password file, he gets into the administrator's shoes and hacks the website. *A case has been registered against the hacker under section 67 of Information Technology Act – 2000 and under various sections of Indian Penal Code.*[20]

2.3 Online Obscenity & Pornography:

Sec. 67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeal to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished 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.

In internet related Cyber Crimes, Obscenity and Pornography poses a major challenge, especially in societies where moral standards are held as the core value of culture and reinforced by religious values. The standard of such morals vary from society to society and even in a given society undergoes substantial changes. But for the moment the law relating to obscenity and pornography of a given system holds steadfast and attempts to regulate the same. Regulating obscenity in a physical world itself is fraught with many difficulties and in Internet it becomes very porous due to its nature of operations. The whole gamut of obscenity and pornography also becomes a lucrative business in Internet as it is banned in most parts of the world and hence a huge market. In countries like United States there had been attempt to curb pornography especially that of the child pornography through acts likes Communications Decency Act of 1996.

The Internet Corporation for Assigned Names and Numbers (ICANN) has given the .XXX top-level domain (TLD) its final approval in March, 2011. The TLD is meant to give pornographic websites a

[20] http://cybercellmumbai.gov.in/html/case-studies/hacker-hacks-into-a-financial-website.html.

clearly marked place/home on the Internet. It has gone through so many ups and downs over the last 11 years and it has finally gone through. The measure had to face a stiff opposition. Nine ICANN board members voted in favor of .XXX, while three members opposed and four abstained. Some countries expressed shock over this development. If we have a look at the journey, ICANN's board of directors rejected .XXX proposal in 2006, the matter of concern was that the TLD might make ICANN responsible for enforcing laws and regulations over Internet porn. However, supporters of the domain brought it back for consideration in 2007 and again in 2010. The TLD got preliminary approval in June of 2010. The proposal is the same as the one outlined in late 2010 that ICM Registry will manage the .XXX suffix, and those looking to register an .XXX domain must first complete an application process that will be overseen by the International Foundation for Online Responsibility (IFFOR).

Section 67 of the IT Act lays down the law that obscenity is an offence when it is published or transmitted or caused to be published in any electronic form. The expressions, 'publishing' or 'transmission' have not been specifically defined under the IT Act, but in Taxmann's commentary under the IT Act, 'publishing means making information available to people'. The commentary also states that 'transmission' and not mere possession, of obscene information is an offence. Transmission may be addressed to an intended recipient for his personal use. But that is not relevant. The act of 'transmission' is sufficient to constitute an offence under section 67 of the IT Act. Therefore if any obscene material is published or transmitted in any electronic form it is an offence under section 67 of the IT Act. The scope is very wide as far as this section is concerned as the provision covers any digital medium including calculators, washing machines etc.,

The punishment for an offence under section 292 of the IPC is on first conviction with imprisonment (simple or rigorous) for a term which may extend to two years, and with fine which may extend to two thousand rupees, and in the event of a second or subsequent convictions, with imprisonment (simple or rigorous) for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

The punishment for an offence under section 67 of the IT Act is on first conviction with imprisonment (simple or rigorous) 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 convictions, with imprisonment (simple or rigorous) for a term which may extend to ten years, and also with fine which may extend to two lakh rupees.

Test of obscenity:

1. The tendency of the matter charged as obscene is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands such a publication may fall

2. The question whether a publication is or is not, obscene, is a question of fact;

3. If a publication is in fact, obscene, it is no defence to a charge selling or distributing the same that the person so charged was innocent.

Case-1. State of Tamil Nadu vs. SuhasKatti

This is the first case which registered conviction under Information and Technology Act. Accused sent defamatory and annoying message about a divorcee in the yahoo message group. E-Mails were also forwarded to the victim from a false e-mail in the name of the victim. Annoying phone calls flooded believing that she solicited sexual relationship. Accused was her family friend interested in marrying her. Her marriage with another ended in divorce and she refused his proposal. The accused was convicted under sections 469, 509 IPC and 67 of IT Act 2000 First case of conviction under IT Act. (2+1+2 yrs. of Imp concurrent. Rs.500 x 2 fine imposed. Nov 4, 2005, Judge Arulraj, Addl Chief Metro Mag, Egmore.

Indian judgments on obscenity are based on the earliest UK judgment of Regina v Hicklin where the court held –

> *"I think test of obscenity is this, whether the tendency of the matter charged as obscene is to deprave and corrupt those, whose minds are open to such influences, and into whose hands a publication of this sort may fall."*

RanjitUdeshi v. State of Maharashtra17, the accused, in their book shop at Bombay, were found in possession of and in fact, sold D.H Lawrence, Lady Chatterley's lover, (unexpurgated edition) which contained obscene matter. The additional Chief Presidency Magistrate convicted all partners and fined them each Rs.20/- with one week imprisonment in default. The Magistrate held that the offending book was obscene. The Accused approached Bombay High Court through a Revision Petition, which was dismissed. Thereafter, the Supreme Court was approached, by means of Special Leave Petition. Dismissing the SLP, the Supreme Court held as under. Obscenity means something which is offensive to modesty or decency, lewd, filthy and repulsive.

This judgment became the basis in the case of where Hon'ble Justice Hidayatullah held that

"We do not think that it should be discarded. It makes the Court, the judge of obscenity in relation to an impugned object to deprave and corrupt by immoral influences. It will always remain a question to be decided in each case and it does not compel adverse decision in all cases."

Whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest;

i. *Whether the work depicts or describes, in a patently offensive way, sexual conduct, specifically defined by the applicable state law; and*

ii. *Whether the work, taken as a whole, lacks serious literary, artistic and political value.*

Case 2. *R Basu v National Capital Territory of Delhi and others* [21]

Facts: Mr. Arun Aggarwal, a practicing advocate, filed a complaint before the learned Chief Metropolitan Magistrate (CMM) against Star TV, Star Movies and Channel V, naming persons responsible for the day-to-day affairs of these channels or the various cable operators transmitting these channels. According to the complainant, the obscene and vulgar TV films shown and transmitted through various cable operators amounted to obscenity and, therefore, the accused persons had committed offences under Sections 292/293/294 IPC and under Section 6 read with Section 7 of the Indecent Representation of Women (Prohibition) Act, 1986.

Acting on this complaint, the CMM viewed these films and, on April 9, 1997, ordered a police inquiry into who was responsible for the exhibition of the films. After the police report was received, the complainant was examined on July 17. After hearing arguments, the CMM passed an order on September 24, 1997, prima facie finding that the four films shown on these TV channels were obscene. The accused persons were summoned under Section 292 IPC, Section 4 read with Sections 6 & 7 of the Indecent Representation of Women (Prohibition) Act, 1986 and Section 5A read with Section 7 of the Cinematograph Act, 1952. The accused filed this petition before the Delhi High Court challenging this summoning order.

The petitioners argued that two of the movies had been awarded “A” certificates by the CBFC and therefore were immune from being prosecuted for obscenity under Section 292 of the IPC and the Indecent Representation of Women Act. With regard to the other two movies it was admitted that they have no censor certificates. However, they stated that with respect to the movie, *Big Bad Mama*, the

[21] 2007CriLJ4245

application for certification had been made to the CBFC. They argued that these movies are telecast from other countries via satellite and broadcasters comply with various strict internal codes as well as the statutory codes prescribed by the Broadcasting Authority of the place of uplink. In respect of some of the individual accused persons, it was argued that they were not responsible for the telecast of these movies.

The high court held that for the two films without censor certificates the petitioners could not claim immunity from Section 292 IPC. For the other two films, also, the court said that, since the petitioners had not produced CBFC certificates, they could not claim immunity from prosecution.

The court observed that the legislature had enacted the Cable Television Network (Regulation) Act to tackle the "problem" of obscenity, and a Programme Code had also been introduced. "Various statutory safeguards for regulating transmission on cable television networks in India have been provided therein. The petitioners have to abide by these guidelines and laws relating to the electronic media, keeping in mind the sentiments and social value of the Indian society, while relaying its programmes."

The court observed that, in view of this development, a joint application was moved by the petitioners and the complainant, in which the complainant agreed not to press his complaint in view of the aforesaid statutory provisions and other provisions now in place.

The issue is which material can be considered as obscene, because standards of obscenity vary with the culture and social ethos. Hence IPC and Supreme Court in Ranjit Udeshi case laid down the test. The same test of "any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it" is deemed to be obscene.

Indian Penal Code Section 292 deals with obscenity**:**

Sec. 292- who ever

(a) sells, lets to hire, distributes, publicly exhibits, or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces, or has in his possession an obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) imports, exports or coveys any obscene object for any of the purposes aforesaid, or knowing or having reasons to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that nay obscene objects are , for any of the purposes aforesaid, made, produced, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person, or

(e) offers or attempts to do any act which is an offence under this section,

shall be punished with imprisonment of either description for a term which may extend to two years and with fine which may extend to two thousand rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

However this section does not extend to—

(a) any book, pamphlet, paper, writing, drawing, painting, representation or figure-

(j) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, are of learning or other objects of general concern, or

(ii) which is kept or used bona fide for religious purpose:

(b) any representation sculptured, engraved, painted or otherwise represented on or in-

(i) any ancient monument within the meaning of the Ancient Monuments and Archaeological States and Remains Act, 1958, or

(ii) any temple or any car used for any conveyance of idols, or kept or used for any religious purpose.

Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offer or attempts so to do, shall be punished on first conviction with imprisonment of either description for a term of which extend to three years, and with fine which may extend to two thousand rupees, and in the event of a

second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees.

Section 294- whoever to the annoyance of others:

(a) does any obscene act in any public place, or

(b) signs, recites or utters any obscene songs, balled or words in or near any public place, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine or with both .

To define obscenity certain tests were laid down by Supreme Court which are applicable to online obscenity or cyber obscenity as well.

2.4 Child Pornography:

As computers and the Internet become ubiquitous, children have increasingly become exposed to crimes such as pornography and stalking that make use of their private information. The newly inserted section 67B of the IT Act (2008) attempts to safeguard the privacy of children below 18 years by creating a new enhanced penalty for criminals who target children.

Sec. 67B :

Whoever,

(a) publishes or transmit or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces 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; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

Punishment for publishing or transmitting obscene material in electronic form: Punishment for publishing or transmitting of material depicting children in Sexually explicit act, etc., in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form—

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes.

Explanation- For the purposes of this section "children" means a persons who has not completed the age of 18 years.

The section firstly penalizes any person who "publishes or transmits" any material which depicts children engaged in sexually explicit conduct, or anyone who creates, seeks, collects, stores, downloads, advertises or exchanges this material would be punished with imprisonment up to five years (seven years for repeat offenders) and with a fine of up to Rs.10 lakh.

Secondly, this section punishes online enticement of children into sexually explicitly acts, and the facilitation of child abuse, which are also punishable as above.

Viewed together, these provisions seek to carve out a limited domain of privacy for children from would-be sexual predators.

The section exempts from its ambit, material which is justified on the grounds of public good, including the interests of "science, literature, art, learning or other objects of general concern". Material which is kept or used for bona fide "heritage or religious purpose" is also exempted.

Despite its various benefits, Internet has provided paedophiles with a new tool. This medium is now being used by child pornographers to lure and prey on children by distributing materials through online chat rooms. This crime may be more difficult to detect when it is done on the Internet as paedophiles may use sophisticated encryption to hide their activities. An example is the September 1998 incident when 180 members of an Internet pornography ring were arrested after an international police

operation involving 12 countries. This massive collective arrest, which included seven British men, cracked down on what was known as the 'Wonderland Club'."

Not only 'publishing' or 'transmitting' of pornographic content involving children, constitute offences, but also its collection, online viewing, downloading, promotion, exchange and distribution.

Case-1. Bombay Case:

The couple, Wilhelm Marty and Loshiar Lily Marty were arrested in Hotel Resort in the northern suburbs of Mumbai, caught red handed by the sleuths of the Crime branch of the Mumbai Commissionerate while they were in the process of recording pornographic films with the children. The panchnama of the room clearly indicated the modus operandi of the couple. Lots of colourful clothes, toys, games and stuffed toys along with an assortment of chocolates, candy and other goodies formed most of their baggage. They could easily pass-off as a package that a well meaning old couple would carry as giveaways to kids. But the baggage also had lots of very sexy lingerie which would otherwise have been the much-prided possession of a bridal trousseau but they were all in children's sizes!! The couple also had lots of condoms, gels and lubricants used during sexual acts, a neat first aid kit and Lily's nursing skills to heal the physical wounds of the kids they were sexually abusing.

When the police got there, Wilhelm Marty was perturbed about nothing, stark naked he walked around the room till he was reminded to wear his clothes. However, he kept heading for his laptop, that was connected to the digital camera and which lay on the study table next to the dresser and opposite the bed.

The couple was very well acquainted in dealing with children as they could communicate at ease with the kids. The two girls aged 9 and 11, who were also present there, in spite of not knowing the language of the Martys, appeared to be quite comfortable. They were telling the parents of these girls that they are an old couple wanting to adopt children but are unable to do so because of the laws of India. But they want to love these poor kids and therefore come to India every year to spend some time with them and give them a good time. Their itinerary showed that they were to take different kids on different days including male children, on all days of their stay in India except on 25 December and they were scheduled to leave the country around 9 January 2001.

The couple was arrested by the police. At the time of arrest, when the police was searching the possessions of the couple, Wilhelm Marty tried to chew a small piece of chip which was in his wallet. It was probably a digital chip that he used in his camera. He was charged with trying to destroy evidence as well.

On 17 December, the couple was produced before the Esplanade court, Mumbai. Thereafter they were in the police custody for two weeks, following, which jail custody was ordered and further investigations were carried out. But investigations showed that the couple actually led a pretty isolated kind of existence. Also, the couple hired private vehicles whose driver was connected with the couple and therefore any child who created any problems was immediately sent back to her family in order to avoid any messy scenes at the hotel.

Before the charges in the case were filed, the police from Switzerland came down to Mumbai. They also brought with them documentary evidence found at their residence in Steinhausen, Switzerland. The couple had however made applications for bail on three occasions and all of them were rejected by the Magistrates court. Later the case was transferred to the Sessions court where again all bail applications were rejected. Finally, in February 2003 the trial began. Finally, on 28 March the final order and judgment were pronounced in the case by Honourable Justice M R Bhatkar- seven years of rigorous imprisonment and an amount of Rs. 5000/- for the girls.

The Honourable High Court of Mumbai had reduced the term of the Marty couple who had offered to pay all the 6 victims on record a sum of Rs.1 lakh towards compensation. The appeal was rejected by the Honourable High Court and Advocate General himself took the decision of moving the Apex court to challenge the release of the couple on behalf of the State of Maharashtra. The case is to be heard by the Honourable Supreme Court but meanwhile the Martys have been granted bail.

2.5 Cyber stalking:

Sec. 66A. *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, (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 fine.

'Explanation.— For the purpose 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, images, audio, video and any other electronic record, which may be transmitted with the message.

The terms 'cyber stalking' and 'internet harassment' are used interchangeably since it is felt that all forms of stalking involve an element of threat or aim to cause the victim distress. This is not considered unreasonable given the meanings commonly attached to terms such as 'stalking' and 'harassment'. For instance, Burgess and Baker offer the following description: 'Stalking, in contrast to a direct physical attack, involves pursuit of a victim and is the act of following, viewing, communicating with, or moving threateningly or menacingly toward another person.' Similarly, the Cambridge International Dictionary defines harassment as 'to make (someone) anxious and unhappy by causing them problems' whilst the online and Concise Dictionary defines harassment as 'to pester, torment or trouble someone by continually questioning or attacking them[22].

- Cyber stalking is the use of the internet, e-mail or other electronic communication devices to stalk another person.

- Repeated threatening, harassing phone calls, sending harassing messages or objects or even destroying victim's property.

- Track their targets through the net in chartrooms, message boards, newsgroups or even mailing lists in which their victims actively take part, befriending their target's friend's to get more information about victims.

- IT Act does not directly address cyber stalking. This problem is considered as an intrusion on to the privacy of individual and sec 72 of IT Act is used to deal with it. Sec 509 of IPC deals with the offence which reads "word or gesture or sound or any gesture or object shall be seen, by such woman or intrudes upon the privacy of such woman shall be punishable with imprisonment up to one year and fine. As sec 509 considers it as intrusion into the privacy sec 72 of IT act is used for this purpose.

- Ritu Kohli (2003), registered first cyber stalking case in India. A friend of her husband gave her phone number and name on a chat site for immoral purposes. Being a computer expert, Kohli was able to trace the culprit. Trial began for "outraging the modesty of a woman", under Section 509 of IPC.

[22] 76 Police J. 204 2003.

- In 2008 Amendment Act Government of India took steps to remedy the situation and introduced sec 66 A to IT Act "Punishment for sending offensive messages": Messages sent to cause annoyance, inconvenience, deceive, mislead, insult, cause injury, intimidation, enmity or hatred through a communication service etc., electronic mails, computer resource, is punishable by imprisonment up to three years and fine.

- This section is aimed at penalizing offences such ad cyber stalking, threat mails, phishing mails

- The provision says that if any mail contains information which is offensive, false, causes obstruction, insult, injury, inconvenience to any person is punishable with maximum three years of imprisonment and fine.

- Criticism: words used in the provision such as "inconvenience", "menacing character" are having potential to be misused for broad interpretation. Words such as 'Annoyance',' obstruction' are not defined in the Act. For example if a sister writes to her brother that She will kill him if he doesn't gift her an IPOD, in a mail it falls in the ambit of this provision very well.

Illustrations:

- In 2009, a 15-year-old Bangalore teenager was arrested by the cyber-crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late.

- According to police officials, at around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials[23].

- Sixteen-year-old Rakesh Patel (name changed), a student from Ahmedabad, sent an e-mail to a private news channel on March 18, 2008, warning officials of a bomb on an Andheri-bound train. In the e-mail, he claimed to be a member of the Dawood Ibrahim gang. Three days later, the crime investigation cell (CCIC) of the city police arrested the boy under section 506 (ii) for criminal intimidation. He was charge-sheeted on November 28, 2008. Status: Patel was given a warning by a juvenile court

[23] Hafeez, M., 2009. Crime Line: Curiosity was his main motive, say city police. Crime Line. Available at: http://mateenhafeez.blogspot.com/2009/05/curiosity-was-his-main-motive-say-city.html [Accessed March 23, 2011].

- A 14-year-old Colaba boy sent a hoax e-mail to a TV channel in Madhya Pradesh, three days after the July 26, 2008, Ahmedabad bomb blasts. He claimed that 29 bombs would go off in Jabalpur. He was picked up by officers of the anti-terrorism squad (ATS) who, with the help of the MP police, were able to trace the e-mail to a cyber café in Colaba. Status: No FIR was registered. The Cuffe Parade police registered a non-cognizable (NC) complaint against him, and the boy was allowed to go home after the police gave him a "strict warning".

- Shariq Khan, 18, was arrested in Bhopal on July 26, 2006, for sending out three e-mails claiming to be a member of the terrorist organisation, which the police believed was behind the 7/11 train bombings. He was arrested by the Bhopal police. Later, the ATS brought the boy to Mumbai and also booked him for a five-year-old unsolved case where an unknown accused had sent e-mail warnings to the department of Atomic Energy (DAE) in 2001. Status: The police filed a charge-sheet against Shariq who claimed that he had sent the e-mails for fun. Trial is pending in a juvenile court. Shariq is presently out on bail in Bhopal.

- On February 26, 2006, a 17-year old student from Jamnabai Narsee School called an Alitalia flight bound to Milan at 2 a.m. telling them there was a bomb on board. He wanted to stop his girlfriend from going abroad. She was one of the 12 students on their way to attend a mock United Nations session in Geneva. Status: After being grilled by the police, he was arrested, but let out on bail.[24]

2.6 Theft of Identity:

The following are provisions relating to data theft or "data crimes" or "data related crimes". Earlier data theft was forcibly brought under sec 66 of IT Act, which is meant for Hacking. But now, 2008 amendment to the IT Act introduced new offences in Sections 66A to 66F. Section 66C is titled 'Punishment for identity theft', and Section 66D is titled 'Punishment for cheating by personation by using computer resource'. These two sections cover the offence of identity theft and identity fraud by use of Internet.

Sec.66B: Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. Under this section, an individual who receives a stolen

[24] Internet Society of India.

computer, cellphone or any other electronic device fitting the definitions contained within the Act maybe imprisoned for up to three years. This offence is different from the offence "dishonestly receiving stolen property" recognized by Sec 411 of IPC because computer source has been defined to include 'data' according to Sec 2(i)(K) of IT ACT which says that computer resource means computer, computer system, computer network, data, computer data base or software. This provision is meant to protect e-commerce and e-transactions involving informational exchange and electronic data exchange. Offences such as misuse of devices with respect to sale, procurement, import and distribution is criminalised in this provision.

Sec.66C: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Sec.66D: Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Sec.66 read with Sec.43(b):Whoever downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, without the permission of the owner/person incharge, is liable for imprisonment upto three years or with fine upto rupees five lakhs or with both.

Sec.66 read with Sec.43(h):Whoever 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 without the permission of the owner/person incharge, is liable for imprisonment upto three years or with fine upto rupees five lakhs or with both.

Identity theft occurs when one's identity is wrongfully appropriated by another. Other types of identity theft in cyber space are cross-site scripting, IP spoofing, and page jacking. Cross-site scripting occurs when code is placed into a web site to force it to send out information against the will of its owners. With IP spoofing, a perpetrator, using software, impersonates a computer trusted by the victim.

As a result, the attacker computer believed by the victim computer to be a different, friendly computer achieves entry into sensitive areas or even control of the victim computer by operating privileged protocols. Jacking occurs when a link, logo, or other internet address is reprogrammed to bring a customer not to the intended site, but to some other one. Phishing is one of the prominent forms of identity theft.

The biggest case of data breach/data theft/identity theft was exposed in January 2009 in which Albert Gonzalez, a 28-year-old American along with his two Russian accomplices, were arrested for masterminding a global scheme[25] to steal data of more than 130 million credit and debit cards by hacking into the computer systems of five major companies including Hannaford Bros Supermarkets, 7-Eleven and Heartland Payment Systems, a credit card processing company.[26] Gonzalez has been said to be one of America's cyber-crime kingpins, by prosecutors.[27] Previously, he was alleged to be the kingpin who masterminded a data breach of over 40 million credit card numbers from TJX Cos and others, causing the parent company of TJX Maxx retail chain, losses of about US$ 200 million.[28]

Sometimes, however, it may not be made for financial gain but as an act of vindictiveness or revenge or obscenity. Suppose if a person has an account with Facebook where her profile with photos and personal details is posted, and one day she is informed by her friend that while surfing Facebook he found her profile with her name and personal details with a lot of pornographic content with obscene language. Here, the thief has committed the theft of her profile with photos and personal details and by using the stolen profile created an obscene profile posing as her. In fact, such instances are not rare. In India, in Gurgaon only, 70 cases of identity theft and fake social networking profiles have been registered till now in 2012.[29]

Phishing: It is one of the forms of identity theft. The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else's login credentials to gain access to protected systems, or by the

---

[25] Michael J. Sullivan, *Hacker charged with providing Data Theft tool in National Identity Theft case*, DEPARTMENT OF JUSTICE, *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2008/wattCharge.pdf (last visited, 6-11-2012).

[26] Kim Zetter, *TJX Hacker Gets 20 Years in Prison*, WIRED, *available at* http://www.wired.com/threatlevel/2010/03/tjx-sentencing/ (last visited, 6-11-2012).

[27] James Gordon Meek & Corky Siemaszko, *'Soupnazi' hacker Albert Gonzalez went from nerdy past to life of sex, guns and drugs*, NEW YORK DAILY NEWS, *available at* http://articles.nydailynews.com/2009-08-19/news/17931753_1_card-numbers-hacking-stephen-watt (last visited, 7-11-2012).

[28] Kim Zetter, *TJX Hacker Was Awash in Cash; His Penniless Codor Faces Prison*, WIRED, *available at* http://www.wired.com/threatlevel/2009/06/watt (last visited, 7-11-2012); Jaikumar Vijayan, *TJX data breach: At 45.6M card numbers, it's the biggest ever*, COMPUTERWORLD, *available at* http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever (last visited, 6-11-2012).

[29] Leena Dhankhar, *Identity Theft cases on the rise*, HINDUSTAN TIMES GURGAON, September 18, 2012, *available at* http://www.hindustantimes.com/India-news/Gurgaon/Identity-theft-cases-on-the-rise/Article1-931638.aspx (last visited, 7-11-2012).

unauthorized application of someone else's digital signature in the course of electronic contracts. Increasingly a new type of crime has emerged wherein sim cards of mobile phones have been 'cloned' enabling miscreants to make calls on others' accounts. This is also a form of identity theft.

For instance, an Indian married couple in US, Amar Singh and Neha Punjabi-Singh, were part of what was called as the largest and most sophisticated identity theft case ever seen in the US, a $ 13 million scam.[30] Amar Singh was one of the four enterprise bosses in this scam where identity theft was done on a large scale, by way of skimming of credit cards as well as by phishing through internet. These identities were sold to different people to stay at five-star hotels or rent high-end cars or even a private jet! With the remaining stolen identities, a network of shoppers was employed which used to shop for high end products, which would reach the enterprise boss, who would then sell it to a person networked person, or 'fence', at a discounted price. Those products sold to fences would then be sold to the general public by retail or otherwise.[31] The various purposes of phishing and the scale would distinguish its various forms and the legal approach should be determined accordingly.

Phishing is broadly of three types:[32]

- **"Dragnet" method** – e-mails are sent with falsified corporate identification, directing a large class of people to web-sites with similarly falsified identification. In this method, specific prospective victims are not identified in advance, but false information is conveyed to trigger immediate response from the victims.

- **"Rod-and-Reel" method** – specific prospective victims are identified in advance and false information is conveyed to trigger responses.

- **"Lobsterpot" method** – web-sites similar to legitimate corporate web-sites that a narrowly defined class of victims are likely to visit, are created. A smaller class of prospective victims are identified in advance, who are induced to give personal information about themselves.

Modus operandi of Phishing: An unwary internet banking customer of a financial institution receives an E-mail purportedly from the institution, which warns the customer that their internet banking privileges will be revoked due to a long period of inactivity—unless they confirm their login name, password, date of birth and other "security" details so that the same can be "updated" on the Institution's

---

30 Allie Compton, *Largest Identity Theft Case In U.S. History: Amar Singh And Wife, Neha Punjani-Singh, Plead Guilty To Massive Fraud*, July 8, 2012, *available at*http://www.huffingtonpost.com/2012/08/07/largest-id-theft-in-history_n_1751241.html (last visited, 6-11-2012).

31 Richard A Brown, 111 *Individuals Charged in Massive International Identity Theft and Counterfeit Credit Card Operation Based in Queens*, October 7, 2011, *available at*http://www.wired.com/images_blogs/threatlevel/2011/10/Operation-Swiper.pdf (last visited, 6-11-2012).

32 VIVEK SOOD, *supra* note 13, at pp. 144-145.

server. Tens of lakhs of such e-mails, ostensibly from a reputed financial institution are sent to people at large, hoping to catch some of the legitimate, gullible customers of that financial institution. A database of valid e-mail addresses is separately harvested by the accused over a period of weeks or months in advance. Such an E-mail contains a clickable URL or a link, which promises to take the Customer to the Internet Banking interface of the Institution.

The moment an unsuspecting customer clicks on such a link, they are taken to what is known as a "spoofed" webpage, which the fraudsters have created. This webpage has the branding & colour-scheme, i.e. feel & look of the genuine institution's internet interface. The URL or web-link address of such dummy Webpages is created by accused on freely available web-hosting servers, and is disguised to appear real. For example, if a person's bank's actual internet presence is on the URL www.myownbank.com, the fraudsters would create a webpage in the fashion www.myownbank.net or www.myownbank.org etc. Any person who submit their actual login details, are not aware that the same are captured in the background by the fraudsters. Such spoofed websites remain active only for a few hours, till the fraudsters have collected the login & password details of a number of several customers who have bitten the bait. Accused then log-in remotely into such victims' accounts and transfer funds into an account opened by them using forged documents, or into the accounts of "Mules" recruited by them with the lure of financial rewards, and using social networking skills. The mules are typically university or college students, or people in debt, or other people who have recently lost their job and thus the source of livelihood or other individuals with a financial crunch. The middlemen or the "mules" may even be paid an advance and then are asked to transfer the funds further through the internet into accounts at other branches, or sometimes even with other banks. Such funds are then accessed by the accused remotely through ATM/ Debit cards or moved around illegally through money transfer services or hawala channels. The account-holder victims only realize that something is amiss, when they receive their bank statements and see funds transfers that they did not do, or when their cheques are returned for insufficient funds. But by the time corrective action can be applied, the conmen have had enough window of opportunity to do a disappearing act. The other type of victims – the mules are the ones who fall into the police dragnet as links in the e-crime. The main perpetrators are often relaxing tens of thousands of miles away. Another variant of Phishing attacks credit card holders of various banks. Legitimate customers receive a warning mail ostensibly from their Bank, advising them that a large number of suspicious transactions have been noticed on their credit card, and thus they would be required to confirm their actual card details, including the 3 digit security code (called CVV- Card Verification Value) indent-printed on the signature stripe of the Card. A spoof web link embedded within the mail would then land the cardholder on the spoofed website, where the sensitive information is captured by the accused. Such credit card account information is then used by the fraudsters to order electronic goods, mobile-phones or other expensive items having a resale value, through mail orders or internet orders. Such shipments are

asked to be delivered at a mail-drop address and collected by the scammers to be sold in the grey markets – at massive discounts – for cash. Yet another variant of the scam asks the e-commerce merchant to process a refund into another card account- which is then used by the accused at another geographic location in a face-to-face environment, at times with conniving merchants.

A recent disturbing trend of Phishing has emerged. It is called "Vishing" – or Voice Phishing. Somebody appearing to be from your Bank either calls you, or you are asked to dial a number of their "Customer Service" or "Fraud Control" department. A hijacked phone-line then connects the caller to what appears to be the original Bank's phone-banking unit. The customer hears a prompt to key-in their card number and other details into the Interactive Voice Response mechanism. These pip-tones are captured and converted into tangible information, which is used by criminals to make internet purchases and fraudulent transactions later billed to customers.

Some recent Phishing scams:

- **RBI Phishing Scam**: The phishing email disguised as originating from the RBI, promised its recipient prize money of Rs.10 Lakhs within 48 hours, by giving a link which leads the user to a website that resembles the official website of RBI with the similar logo and web address. The user is then asked to reveal his personal information like password, I-pin number and savings account number.

- **IT Department Phishing Scam:** The email purporting to be coming from the Income Tax Department lures the user that he is eligible for the income tax refund based on his last annual calculation, and seeks PAN CARD Number or Credit Card details.

- **ICC World Cup 2011:** In this scam, the internet users of the host countries i.e. India, Bangladesh and Sri Lanka where the matches of the world cup were going on were specifically targeted by fraudsters. The Modus Operandi was similar to the banking phishing attack. The fraudsters through the similar looking fake website of organizers of the event tried to lure victims with special offers and packages for the World Cup final. The Users were asked for credit card details to book tickets and packages along with their personal information which once submitted would be used to compromise the online banking account of the victim leading to financial losses to the victim.

- **Google:** Recently, the users of the Google email services, "Gmail" purportedly received a legal notice from the Gmail team which wanted users to refurbish their account name, password, occupation, birth date and country of residence with a warning that users who did not update their details within 7 days of receiving the warning would lose their account permanently. However, the

spokesperson of the Google denied any such legal notice coming from them and stated it to be a phishing attack designed to collect personal information, called 'spoofing' or 'password phishing'.

Phishing has become a concept well discussed in Indian Courts by now. In *National Association of Software v. Ajay Sood and Ors*,[33] court elucidated the concept of phishing as a cybercrime wherein criminals aim to defraud people using computers and internet by pretending as genuine entity such as a bank to extract personal sensitive information including password and credit card details and misuse the same for making wrongful financial gains. In *Shri Umashankar Sivasubramanian v. ICICI Bank*,[34] petitioner filed a case for compensation under Section 43 wherein petitioner was victim of phishing attack through impersonating email that appeared to be bank's official communication asking him to update his personal account information. The bank took defence that the plaintiff was negligent. The court held that bank had not adopted due diligence measures in securing its internet banking system in such a manner that a customer would recognize a mail from the bank and directed it to pay sum of rupees 12,85,000/- as compensation to the petitioner.

2.7 Cyber Fraud :

Frauds[35] committed through Internet are done in various methods and the legitimate online businesses of banking and insurance are the one, which bears the brunt of the cyber crime. The fraud in the cyber world is committed against individuals as well as by individuals against corporations against government services. The Fraud in Internet in the individual scale will include e-mail soliciting of fund transfers, sale of products, services that will entice the potential victim of his personal details of bank accounts, credit cards and other details, which will be used to commit the fraud against the individuals. On the corporate side, mostly in banking and financial sectors, individuals commit fraud on online transactions and services.

In a recent survey by the Computer Security Institute of USA[36] it was found that based on responses from 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2002 Computer Crime and Security

---

33 119 (2005) DLT 596.

34 Petition number 2462/2008 before Adjudicating Officer at Chennai, *available at*http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf (last visited, 8-11-2012).

35 Fraud -The word "fraud" generally describes deception that results in monetary profit (as opposed to other types of deception). Most computer hacking is better labeled "abuse" rather than "fraud". Example: telecom fraud (toll fraud) Most fraud available to hackers involves defrauding the telephone system. satellite TV fraud Getting satellite for free. credit card fraud Using credit cards, especially to access graphically oriented sites

36 The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

In the Indian context the IT Act has no provisions nor has dealt with cyber frauds except for frauds relating to e-commerce related accounts of subscribers holding digital signature under section 44 of the IT ACT which is not a criminal liability. However the acts of fraud through Internet can be covered through the sections of 25 and 415 of the Indian Penal Code. Though the exact use of word of 'fraud' is debatable, the acts can be covered under 'cheating' by section 415 of IPC, which states:

> **Sec. 415B Cheating:** *Whoever, by deceiving any person, fraudulently, or dishonestly induces the person so deceived to deliver any property to an person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".*

Thus the commonly used term of 'fraud' can be brought under cheating if it fulfills the following aspects of:

1. A false representation of a person which he or she knows is false at the time of the representation

2. The intention of the representation is dishonest with a motive of deceiving the person to whom it is made and

3. The person is deceived to part away with a property or an omission, which otherwise he or she would not have done without the deception.

The following are other provisions which have bearing with Frauds committed in cyber world.

Sec. 25- Fraudulent Act*: Section 25 of I.P.C., there is a mention of the word 'fraudulently' which states that, 'A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise". Here again the word 'defraud' is not defined but is interpreted by Courts*[37] *in various cases. Here deception is an essential element of fraud and it does not matter whether it is for an advantage of from ill will towards the person deceived. Thus frauds involved in Internet can evoke section 25 of I.P.C.*

[37] Sir James Stephen in his 'History of Criminal Law of England' defines the word 'defraud' as consisting of the elements a0 deceit or an intention to deceive or in some cases mere secrecy, and b) either injury or possible injury or an intent to expose some person to any such injury by such deceit or secrecy.

Sec.416 ***Cheating by Impersonation:*** *A person who a) pretends to be some other person or b) by knowingly substituting one person for another or c) by representing that he or any another person is a person other than he or other person really is. The person may be real or imaginary one. Thus a person committing fraud in online transaction of a banking account will evoke section 416* [38] *for cheating by personation.*

Secs. 417- 420 Aggravated Cheating: *Here further section of 418 will apply for cheating with knowledge that wrongful loss may thereby be caused to a person whose interest the offender is bound to protect. Further cheating and thereby dishonestly, inducing the person deceived to deliver any property to any person, or to make, alter, or destroy a valuable property to any person, or to make, alter, or destroy a valuable security or anything which is signed, or sealed and which is capable of being converted into a valuable security will apply for 'fraudulent acts' in the cyber space.*

The following is the provision dealing with cyber fraud in Information and Technology Act:

Sec 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 Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a terms which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 71 of the Act provides that if a person obtains a license or Digital Signature Certificate from the Controller or Certifying Authority, as the case may be, by any misrepresentation or by suppressing any material fact, he shall be punished. Punishment: The punishment shall be either imprisonment for a term which may extend to two years or fine to a tune of one lakh rupees or both.

Publishing false Digital Signature Certificate

Publishing for a false digital signature certificate or making false digital signature certificate available by any other means to any other person is an offence. However, this offence is not strict but depends upon the knowledge of the accused. An accused will be liable for only when he has knowledge that-

a) the certifying authority listed in certificate has not issued; or

[38] S 416- should have at least one requirement of 1) pretension of a person as another person 2) such substitution is with full knowledge and 3)such representation of himself or any other person than he or such person really is.

b) the subscriber listed in the certificate has not accepted it; or

c) the certificate has been revoked or suspended.

Unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Punishment:

Any person who publishes a false Digital Signature Certificate or otherwise makes such certificate available to any third 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.

Publication for fraudulent purpose:

Any person, who knowingly creates, publishes or otherwise, makes available a digital signature certificate for any fraudulent or unlawful purpose 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.

2.8 Mischief

The major threat to the cyber world is that of the 'Virus'[39]. The computer virus is like that of the biological virus which can replicate, spread throughout the network it travels and destroys the valuable data, disrupts programmes and may cause havoc to vast number of computers. Computer viruses are also programmes that attach with the host computer without the user's knowledge and carry out the functions intended by the creator. The virus is also programmed in such a way that it damages data by Data Diddling, Trojan Horses or Logic Bombs.

[39] Virus - A virus is a program (or a fragment of code) that replicates by attaching a copy of itself to other programs. For a virus to be activated, the software it infects must first be run. A biological virus is not a "living" thing. Instead, it is simply a strand of DNA. When it enters a living cell, it takes control of the cell forcing it to generate duplicate copies of the original DNA strand. In much the same way, a computer virus hijacks the computer forcing it to generate duplicate copies of the original virus. Computer viruses are so common because humans do not practice sufficient cyber-hygiene when exchanging files. Key point: An "anti-virus" programs scans the disks on your system hunting down those files that have signatures indicative of infected files. Since file-scanning technology is generic, most anti-virus programs also scan for other hostile content, such as Trojans. The popular use of the word "virus" means any form of malware. For example, in the movie Office Space, the protagonists write what is called a "virus" that runs in the banking mainframe to steal round-off errors. In contrast, the technical definition limits itself to just those forms of contagious malware that spreads by infecting other programs. Viruses have a life cycle from the point they are originally created, distributed, found by anti-virus programs, and then eradicated. They also mutate as script kiddies take viruses, make small alteration that avoids current virus scanners, and redistribute the viruses. Example: boot sector Historically, the most popular kind of virus, though becoming less popular as floppies are used less often. E.g. Form Virus macro virus -Data files cannot contain viruses -- except when they also include scripting "macros". Currently the most popular kind of virus. Most macro viruses are written in Visual Basic, a programming language included as part of Microsoft Office products (Word, Excel). E.g. Marker Virus file infector. The traditional definition of a virus: an executable file contains a virus imbedded within. When run, it attaches the virus to other executables on the system

The viruses today are deployed to attack Internet networks and can be of the types as such as that of – File Infector, Resident Program Infector, Boot Sector Infector, Multi-party Virus, Dropper, Stealth Virus, Companion Virus, Polymorphic Virus and Mutation Engine[40]. The induction of these viruses by legitimate means of e-mail communication will cause damages, which cannot be computed as it depends on its speed. This kind of activity can be equated to that of the offence of mischief. In the physical world 'mischief' is a crime defined by IPC by S 425 and by sections up to 440.

> ***Sec. 425-*** *whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or effects it injuriously, commits 'mischief'.*
>
> *The section to be interpreted that an act to constitute as 'mischief' should have –*
>
> *a) Intention or knowledge of the likelihood to cause wrongful loss or damage to the public or to any person*
> *b) The act causing destruction or damage or alters the property*
> *c) Such act of damage or destruction altering or diminishing the value of the property*

Applying the traditional definition of Mischief under S 425 to spreading of virus will result only in the imprisonment of three months and a fine. However by IT Act such a damage is defined in Sec 43.

> ***Sec 43. Penalty 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, -*
> *(a) Accesses or secures access to such computer, computer system or computer network;*
> *(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;*
> *(c) Introduces or causes to be introduced any computer contaminant or Computer virus into any computer, computer system or computer network;*
> *(d) Damages or causes to be damaged any computer, computer system or Computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;*
> *(e) disrupts or causes disruption of any computer, computer system or computer network;*

[40] Dr. R.K. Tewari, et al, Computer Crimes and Computer Forensics, Select Publishers, New Delhi, 2002

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(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, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Thus the categorization of 'infecting virus in cyber space' fall under mischief, the IPC provisions are ineffective and one need to invoke the IT Act for effective regulation as the damage of this 'mischief' is far beyond expectations than the 'mischief' in the physical world. There are debates whether the intention part of the 'mischief monger' could be stretched to the potential damage than it was intended[41].

2.9 Cyber Defamation

Defamation, which is conventionally associated with 'published materials', assumes significance over the Internet. In order to understand the conventional concept of defamation one need to look into the relevant provision of IPC section 499.

*According to **Sec. 499** defamation has three main aspects of:*

a) Making or publishing any imputation concerning any person,

b) Such imputation must have been made by

i) words, either spoken, or intended to be read; or

ii) signs; or

iii) Visible representation

c) such imputation must be made with the intention of harming or with the knowledge or with reason to believe that it will harm the reputation of that person.

[41] Prosecutors' use of the CFAA is illustrated by the Morris case, which perhaps is the most infamous crime committed on the Internet. On November 2, 1988, Robert Morris sent a computer "worm" across the Internet from the MIT computers. The "worm" replicated itself through the network much faster than Morris had anticipated, and thereby caused an estimated 6,200 Internet computers to shut down. It is estimated that Morris caused some $98 million dollars in damage. If Morris had coded his worm to be destructive, untold additional damage would have been done. Morris was subsequently charged with violation of 1030(a)(5)(A) of the CFAA which prohibits intentional unauthorized access to a federal interest computer with a resulting loss of $1000. Morris's defense was that although he did intend unauthorized access, he never intended to cause damage. But the District Court (and later the Second Circuit) found that intent to access the federal interest computer was sufficient by itself to warrant conviction. Morris was sentenced to three years probation, 400 hours of community service and a fine of $10,500. Ironically, when Morris discovered the damage being done, he considered writing a "worm killer" antidote program, but decided that he had caused enough damage. Although the antidote might have been effective, it also would have exposed Morris to additional criminal liability on a second offense. source- http://www.cla.org/msf_cybercrimes.pdf.

The key element here is that of publication. Again publication is defined as one, which is to a third party, and not a written one to the complainant. Thus a one to one e-mail – from party A to B cannot be brought under defamation. But if A has communicated by e-mail to C about B and it will fall under defamation. For all purposes e-mail of such nature will come under the purview of defamation. In essence any publication which will include e-mail in today's context to a third party other than the person defamed will constitute defamation.

In the cyber world, apart from E-mail, newsletter via Internet, mailing lists, news groups, Usenet groups[42] bulletin boards, websites private or subscriber based will come under the purview of publication and will be liable to be brought under the defamation.

There are also exceptions to the section 499 which are as follows:

1. Imputation of anything true, it be for the public good to make it is not defamation- for this it has to qualify for public good and also what is published should be proved to be true in substance and in fact.

2. It is not defamation to express in good faith any opinion respecting the conduct of a public servant in the discharge of his public functions or respecting his character, so far as his character appears in that conduct and no further- such publication should be correct not only in substance and fact but also should not exceed in its limit.

3. To express in good faith any opinion respecting the conduct of any person touching public questions and respecting his character so far as it appears in that conduct, is not defamation- this is for fair criticism and this should not have fact which are not true and will lose the ground of the fair criticism

4. It is not defamation to publish a true report of proceedings of court or of the result of such proceedings. It need not be verbatim report but a report, which is substantially true.

5. It is not offence to express in good faith any opinion on the merits of a case decided in court or the conduct of witnesses and others concerned or respecting the character of such persons so far

[42] USENET - Point: The protocol for transporting USENET messages is called NNTP: "Network News Transport Protocol". The USENET is often applied to NNTP servers in order to stop the flood of Spam. It is often applied to ISPs who allow users to send lots of Spam or allow their servers to be hijacked. For this reasons, many ISPs (especially high-speed cable modem and DSL providers will scan their customers looking for unauthorized NNTP servers. USENET presents a philosophical challenge to the Internet because of its distributed nature. It allows anonymous publishing of material that cannot be traced back to the source. This challenges the historic concepts of intellectual property and how it can be protected. For example, when RC2 and RC4 were posted to USENET, they stopped being trade secrets.

as it appears in that conduct- freedom to discuss fairly on the administration of justice but should be fair and honest, reasonable in its analysis.

6. It is no offence to express in good faith opinion or the merits of any performance which its author has submitted to the judgment of the public or respecting the character of the author so far it appears in such performance - any comment on the literary or artistic work, if it is intended as a valid critique for the consumption of the public and as a guide and judgment to help the public.

7. It is no offence for a person having lawful authority over another to pass censure in good faith - this is on censuring of a higher authority on good faith. An academic head sending a note to be put up in a notice board or censuring a pupil in front of other pupils will not amount to defamation as the academic head derives his authority from the parent to do the act in good faith.

8. It is no offence to prefer an accusation in good faith to an authorized person.- a complaint before a magistrate or an appropriate authority on the actual conduct will not amount to defamation

9. It is no offence if a person makes an imputation in good faith, for the protection of his or others interest. - to protect one's own interests or of others or for public good if it is made in good faith it is an exemption.

10. It is no offence to convey a caution intended for the good of the person to whom it was conveyed or for public good – if someone publishes a matter, which is defamatory to a practice of some people in the community, but in the interest of the members it will not amount to defamation.

All the above exemptions and the provisions of Section 499 will apply to matters published in World Wide Web and also to closed groups of news groups, chat rooms or bulletin board where there is a possibility of the third person viewing the material other than the complainant.

Another aspect of Defamation in the physical world is that of the publisher other than the other if they are different bound by section 501 where anyone publishing with knowledge of the defamatory matter or reason to believe that is aware of such possibility will be liable for imprisonment and fine to the range of two years. Thus the publishers and editors of the physical world would often be liable in defamation suits. In the context of the Internet the website owner and Editor will be liable if they allow their bulletin boards or commissioned articles if they carry defamatory article. However the question is the role of the Internet Service providers (ISPs)[43] who control the flow of the information and also the

[43] ISP (Internet Service Provider)- The ISP provides access to the Internet. The Internet is fundamentally just a collection of ISPs. It is official anarchy: there is no single ISP that controls the Internet, instead the ISPs get together and form agreements among themselves as to how the Internet should operate. Contrast: Today's ISP is often differentiated. Some provide "retail" service to home and business customers at the edge of the networks, others (often called

transmission the information through the network of subscribers. The moot point is whether they will be considered as ‘Publishers’ The argument of the Internet service providers is that they are a technology service providers and do not have the control exercised by News Papers or other media like television. However they are not absolved in total but nevertheless the dynamics of millions of users using their platform also makes it difficult for them to monitory every aspect of information flowing them.

Sec. 79. Network service providers not to be liable in certain cases

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 there under 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;

2.10 Impersonation

Sec. 66D. *Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.*

The basic nature of the crime involves the use of identifying information of someone to represent oneself as the individual for fraudulent purposes, essentially, the wrongful appropriation of one's identity by another. Conventional crimes of identity theft would include forgeries featuring credit cards, thefts and making of false statements, online versions of the same will involve logging into someone's account and making a defamatory statement, online shopping using someone else's credit card etc.

Prior to the amendment act, the crime of identity theft was forcibly brought under S.66 within the ambit of 'hacking', which presupposes that there was an infiltration of a computer resource involving

---

"NSPs" or "network service providers") provide the backbone access to ISPs. Yet others provide primarily web-hosting services. Key point: Many members of the hacking community maintain their own private ISP containing dial-up accounts for neighbors/friends, a couple T1 lines, and a few porn sites. Therefore, when you are attacked from a dial-up user and you complain back to that user's ISP, you may actually be just complaining back to the hacker himself.

'alteration, deletion or destruction' of the information residing therein, facilitating the crime of identity theft. However, under the new provision, S.66C, the means by which the identifying information is accessed is discounted and only the act of making fraudulent or dishonest use of the information itself is criminalised.[44]

2.11 Cyber Terrorism

Section 66F - Punishment for cyber terrorism:

(1) Whoever,-

(A) 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 –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) 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 (B) 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 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.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

[44] Neal K. Katyal, Criminal Law in Cyberspace, 149 (4) U. PA. L. REN. 1027 (2001).

Sec 66F defines cyber terrorism, Any person with an intention to threaten integrity or security of nation denying access to computer source, or penetrating into, or introducing computer contaminant, (B) exceeding the authority to access or unauthorized access to the restricted data with an intention to threaten security, sovereignty etc. punishable up to imprisonment for life

The section is comprehensive in that sub-clause (A) first enumerates the methods by which the act is committed, the wrongful conduct, as it were, and then proceeds to describe the potential damage that may be caused by such acts. It deals with damage to essential supplies and critical information infrastructure.

It is obligatory for the definition to cover acts involving the internet such as money settlement through internet banking, use of internet channels to communicate terrorist plans across countries, hacking and defacement of governmental and non-governmental websites, virus and Trojan attacks aimed at secure infrastructural and cyber assets of the country etc.

Mark Pollitt, special agent for the FBI, defines it as follows: "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents[45]."

Dorothy Denning defines cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives[46]". While R. Stark defines cyber-terrorism as "any attack against an information function, regardless of the means[47]"

Classification of cyber terrorism

This section seeks to enumerate a variety of crimes that are commonly considered act of cyber terrorism. It is important to note here that these acts need to be qualified with sufficient motive and destructive effect to be classified as acts of terrorism. Experts classify cyber terror into three levels-

a) The first level is called the simple structured, wherein the capability of the terror organisation is rather low, they simply use tools of cyber terror that are already available or provided by somebody else.

---

45 Mark M. Pollitt. "A Cyberterrorism Fact or Fancy?" Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289.

46 Dorothy E. Denning. "CYBERTERRORISM" Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University May 23, 2000 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, last visited 22nd September 2012.

47 Rod Stark. "Cyber Terrorism: Rethinking New Technology". Department of Defense & Strategic Studies Graduate Assistant Southwest Missouri State University http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html, alst visited 22nd September, 2012.

b) The second level is the advanced structured, here the organisation has greater mastery over tools of cyber terror, they are capable of running more complex programs affecting multiple systems as well as develop some basic tools themselves

c) The third level is the complex coordinated, the terror groups in this bracket have sophisticated skills to cause failure of multiple systems, and the perpetrators are even able to develop complex tools and programs to serve their purpose.

Following are some of the important cyber terroristic attacks.

a) **Cyber Terrorism of China:**

In 2001 there occurred a mid-air collision between a US surveillance plane and a Chinese fighter plane. This was followed by intense tension and conflict between the two nations, even resulting in a cross fire of hacking, web defacement and other cyber-attacks sponsored by the two governments.

Prominent Chinese hacker groups such as Honker Union of China and Red Guest Network Security Technology Alliance organised a sustained cyber-attack against American cyber infrastructure. Chinese hackers used internet postings and chat rooms to attack US systems, although Chinese government's involvement is unclear, it can be said to have tolerated the attacks if no sanctioned them, since no arrests were made. Approximately 1,200 American websites including those of the White House, US Air Force and Department Of Energy has been subjected to DDOs attacks and defaced with pro-China images.[48]

b) Cyber terrorism of Pakistan:

The number of pro-Pakistan hackers hitting Indian sites has been on the rise over the past three years. The figures stand at 45 in 1999, 133 in 2000 and 275 by the end of August 2001.[49] Pakistani groups such as G-Force and Doctor Nuke are politically motivated and their attacks have been highly visible and involved in information dissemination.

Indian targets have ranged from the Indian Parliament, Zee TV, Asian Age, Indian Institute of Science and the Baba Atomic Centre. (The most worrying attack was when close to 5 megabytes of possibly sensitive nuclear information was downloaded from the server of the Bhabha Atomic Research Centre).

---

48 http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300, last visited 23rd September, 2012.
49 Ibid.

c) Cyber Terrorism of Israel and Palestina:

The Middle East's most long drawn and violent conflict has transcended into cyberspace as well. Cyber-attacks have included web defacement, DDoS as well as worms and Trojans.

In response to the kidnap of 3 Israeli soldiers, pro- Israeli hackers mounted sustained DDoS attacks against the sites of Palestinian authorities. In response the pro-Palestine hackers retaliated by taking down sites of the Israeli Parliament, the Israeli defence forces, foreign ministry, Bank of Israel, Tel Aviv Stock Exchange and other critical infrastructure. Palestinian attacks have been of such intensity to even be dubbed cyber jihad. Palestinians planned to launch a phased attack, phase 1 involves targeting the Israeli government, phase 2 is aimed at the nation's economic infrastructure, and phase 3 is aimed at the nation's major communication infrastructure, while the final phase seeks to hit foreign targets.[50]

d) Cyber terrorism in the South Pole:

From a distant hideout in Romania, a group of cyber terrorists held nations to a ransom, by threatening to cut off the life support system of 58 scientists stationed in Antarctica, who were ultimately saved by efforts of the FBI (Federal Bureau of Investigation, US).

The attack occurred by an intrusion into the network of the National Science Foundation's Amundsen-Scott South Pole Station. The extortionists took possession of certain sensitive information from the network of the South Pole, and threatened to sell it to another nation. To ensure credibility they sent copies of the extracted information to US government. They sent an email to US Antarctic Pole Program and South Pole station which received an e-mail which begins as follows: "South Pole Station Servers HACKED. This is a message from earth to earth, do you copy?"

Cyber forensic experts traced the mail, which was ultimately traced to a cyber cafe in Romania, two persons were suspected and arrested, they are under trial in Romania at the moment.

Later details began to come out of the terrorists possessing the ability to shut off heat to the facilities of the scientists essentially endangering their ability to survive in Antarctica, the computers that were compromised also contained the controlling devices for survival, financial records etc. In a testimony by FBI cyber chief Keith Lourdeau to a US Senate subcommittee conducting hearings on cyber terrorism he stated, "During May, the temperature at the South Pole can get down to 70 degrees below zero Fahrenheit; aircraft cannot land there until November due to the harsh weather conditions." "The compromised computer systems controlled the life support systems for the 50 scientists."[51]

---

50 Id.

51 http://www.theregister.co.uk/2004/08/19/south_pole_hack/, last visited 27th September, 2012.

Luckily the forensics team was able to nab the terrorists before those factors came into play.

e) Cyber Terrorism by Russians :

In the spring of 2007, Estonia was subject to widespread and repeated cyber-attacks in the form of web defacement, DDoS (the terrorists created zombie computers in Egypt and others such far flung places to cause havoc), destruction of Internet Service Provider services. Websites of Estonian government were defaced by posting political messages; websites of critical financial institutions, schools, media channels etc. were also attacked. At one point in time the hackers had disabled the e-mail server of parliament.[52]

The tools used in the attacks were far from new and innovative, they were not even targeted at critical defence or infrastructure, but given the small size of the Estonian nation and its excessive dependence on technology, the impact of the attacks was felt quite a lot. One of the Estonian banks that reported economic impact of the attack estimated a loss of around 1 million. During the duration of attacks, credit cards had to be put out of operation and ATMs stopped working.

The attacks resulted from the Estonian government's decision to move a World War II memorial, the Bronze Soldier, celebrating liberation of Russia from Nazi reign from central Tallinn to a less prominent military cemetery in Estonia[53]. The statue was said to represent Russian oppression to the Estonians. This caused Russian speaking minorities to riot and protest and even launch cyber-attacks against the state of Estonia.

For a long time during and after the attacks there was a lot of confusion as to the nature of the attacks, the Estonian government did not want to give it the status of a cyber-attack and was keen to dub it as a series of hactivisms, however continuous and unrelenting nature of the attacks has made many experts conclude that they constitute a cyber-attack.

The Estonian government was unable to make very many arrests, while speculation was rife of Russian involvement no evidence of this could be gathered even by NATO.

---

[52] http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss&sei-redir=1&referer=http%3A%2F%2Fwww.google.co.in%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dthe%25202007%2520estonia%2520cyber%2520attacks%2520scholar%26source%3Dweb%26cd%3D1%26ved%3D0CCAQFjAA%26url%3Dhttp%253A%252F%252Fscholarcommons.usf.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1105%2526context%253Djss%26ei%3Dfw57UO2LNdDQrQfr7YG4Dg%26usg%3DAFQjCNEUvmtvTxLaJ6Gbd7JPoimCQPanWQ#search=%222007%20estonia%20cyber%20attacks%20scholar%22, last visited 22nd September, 2012.

[53] http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_ the_2007_Cyber_Attacks.PDF, last visited 22nd September, 2012.

Estonian government had to seek the assistance of Finnish, German and Israeli technical experts to get the systems back on track. Help was also provided by the technical division of the NATO and the EU.

Following the attacks, the EU, NATO and Estonia reviewed laws relevant to cyber terrorism and brought about some significant changes. Estonian laws that were amended included the laws relating to cyber security, criminal law and crisis management law. The definitions of crimes were reviewed to ensure that computer related crimes were included in the definitions of crimes; a distinction was also made between calculated acts of cyber terror and normal computer crimes.[54]

At its Summer Summit in 2008, NATO adopted the Policy on Cyber Defence and set up a Cyber Defence authority in Brussels. Tallinn was later, declared the home to the NATO Co-operative Cyber Defence Centre of Excellence.

EU(European Union) released a 'Digital Agenda for Europe' and revealed plans to establish CERTs for EU institutions, conduct cyber-defence simulations, and create a joint European cyber-crime fighting platform.

NATO adopted a new Strategic Concept in Lisbon in November 2011, which sought to develop and strengthen cyber defence weapons.[55] Life imprisonment is the punishment prescribed for this offence.

2.12 Breach of Confidentiality and Privacy:

Section 72 of the Act imposes liability on a person who secures access to any electronic records, book, register, correspondence, information, document, or other material, while exercising powers under the Act, rules or regulations made there under, to maintain confidentiality of such material. He shall not disclose without the consent of the person concerned such electronic record, book, register, correspondence, information, document or other material in person.

Punishment:

Any person who commits a breach of confidentiality or privacy 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.

---

[54] Ibid.

[55] Researcher for cyber terrorism Ms Upasana Rajaram, Vth Year BA LLB (Hons), NALSAR University of Law.

2.13 Offences by Companies:

Section 85 of the Act provides that where a person committing a contravention of any of its provisions of the Act or any rule, direction or order made there under is a company, every person who at the time of the contravention was committed, was in charge of, and was responsible to the company for the conduct of the contravention and shall be liable to be proceeded against and punished accordingly. However, a person shall not be liable if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Where a contravention of any provisions of the Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer, of the company , such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

The company for the purposes of the present provision means anybody corporate and includes a firm or other association of individual's and director, in relation to a firm, means a partner in the firm.

Securing Access to Protected System:

As per Section 70 the Act Any person who secures access or attempts to secure access to a protected system which the appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system in contravention of the provisions of this section is liable.

Punishment:

Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Directions of Controller to a subscriber to extend facilities to decrypt information:

According to Section 69 (1) and Section 69 (2), if the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government

to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

Punishment:

The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

2.14 Punishment for Damage to Computer System:

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - accesses or secures access to such computer, computer system or computer network downloads, copies or extracts any data, computer data base information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; damages or causes to be damaged and computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network; disrupts or causes disruption of any computer, computer system or computer network; denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means; provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or compute network he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

2.15 Liability of Intermediaries:

Who are intermediaries?

Intermediaries are entities that provide services that enable any content that is created on the Internet to be delivered to the user. Let us look at the players involved in this chain:

Internet Service Providers (ISP) – ISPs like Airtel and MTNL help users to get connected to the Internet by means of wired or wireless connections.

Search engines – These are web sites like Google and Bing that help users to search for specific information on the web and provide links to web-sites having content relevant to the search terms given by the user.

DNS providers – These service providers translate the domain names (e.g. www.sflc.in) to addresses (eg.64.202.189.170) that can be understood by computers.

Web hosts – These are service providers like Godaady.com that provide space on server computers to place files for various web sites so that these sites can be accessed by users.

Interactive websites: This includes social media sites like Facebook and Twitter that act as platforms to store and retrieve content, blogging platforms like BlogSpot and Word press, auction sites like eBay, and payment gateways like PayPal. The pictorial representation gives an overview of the intermediaries involved in a common Internet transaction.

Cyber Cafes – The Information Technology Act, 2000 includes cyber cafes also under the ambit of the definition of intermediaries[56].

Countries like the US and members of the European Union now provide protection to intermediaries from such user-generated content. The Digital Millennium Copyright Act (DMCA) and the Communications Decency Act in the US and the Directive on Electronic Commerce in the EU provide protection to intermediaries from liability arising out of content posted by users of their services. Such protection is often termed as a "safe harbor" protection. The following provision of IT Act deals with role and responsibilities of intermediaries.

Sec.79 :

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3) an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

[56] http://www.thehoot.org/web/home/rules.php?cid=16.

(3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.-For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary. Section 79 of the Information Technology Act"

On the 11th of April 2011, the Government of India notified the *Information Technology (Intermediaries Guidelines) Rules 2011* that prescribe, amongst other things, guidelines for administration of takedowns by intermediaries.

The amendment to the provision on intermediary liability (s.79) while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies.

Firstly, the requirement of taking down content upon receiving "actual knowledge" is much too heavy a burden for intermediaries. Such a requirement forces the intermediary to make decisions rather than the appropriate authority (which often is the judiciary). The intermediary is no position to decide whether a Gauguin painting of Tahitian women is obscene or not, since that requires judicial application of mind. Secondly, that requirement is vitiates the principles of natural justice and freedom of expression because it allows a communication and news medium to be gagged without giving it, or the party communicating through it, any due hearing. It has been held by our courts that a restriction that does not provide the affected persons a right to be heard is procedurally unreasonable.

The intermediary loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information. While the first two are required to be classified as true "intermediaries", the third requirement is a bit too widely worded. For instance, an intermediary might automatically inject advertisements in all transmissions, but that modification does not go to the heart of the transmission, or make it responsible for the transmission in any way. Similarly, the intermediary may have a code of conduct, and may regulate transmissions with regard to explicit language (which is easy to judge), but would not have the capability to make judgments regarding fair use

of copyrighted materials. So that kind of "selection" should not render the intermediary liable, since misuse of copyright might well be against the intermediary's terms and conditions of use.[57]

Under the Information Technology Amendment Act, 2008, *Section 79 has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him*. This is however subject to following conditions:

- the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;
- the intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission;
- the intermediary observes *due diligence* while discharging his duties.

As a result of this provision, social networking sites like Facebook, Twitter, and Orkut etc. would be immune from liability as long as they satisfy the conditions provided under the section. Similarly, Internet Service Providers (ISP), blogging sites, etc. would also be exempt from liability.

However, *an intermediary would lose the immunity*, if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act. Sections 79 also introduced the concept of *"notice and take down"* provision as prevalent in many foreign jurisdictions. It provides that an intermediary would lose its immunity if upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act and it fails to expeditiously remove or disable access to that material.

2.16 Cyber Security and India

The Indian Computer Emergency Response Team

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

[57] Short note on IT Amendment Act, 2008, by Pranesh Prakas, http://cis-india.org/ internet-governance/publications/it-act/short-note-on-amendment-act-2008

CERT-In was created by the Indian Department of Information Technology in 2004 and operates under the auspices of that department. According to the provisions of the Information Technology Amendment Act 2008, CERT-In is responsible for overseeing administration of the Act.

In 2004, the government set up the Indian Computer Emergency Response Team (CERT-In). Such set-ups exist in almost 62 countries of the world covering Asia, North and South America and Europe. CERT-In's main task is to ensure the security of cyberspace in the country by enhancing the security of communications and information infrastructure, through proactive action and effective collaboration, aimed at security incident prevention, prediction and protection and security assurance. It has as a stated mission: Alert, Advice and Assurance. In carrying out its mission, CERT-In has viewed its roles in both reactive and proactive modes, besides identifying its reporting, analysis and response functions. CERT-In's four enabling actions include:

1. Enabling the government as a stakeholder to create the appropriate environment/conditions by way of policies and legal/regulatory framework to address important aspects of data security and privacy protection.

2. Enabling user agencies in the government and critical sectors to improve the security posture of their IT systems and enhance their ability to resist cyber attacks and recover within a reasonable time, if attacks do occur.

3. Enabling CERT-In to enhance its capacity and outreach and to achieve force multiplier effects to serve its constituency in an effective manner as a 'trusted agency'.

4. Hold public communication and contact programmes to increase cyber security awareness and to communicate government policies on cyber security.

CERT-In has also circulated security guidelines to all government organisations and made them available on its website as well. The organization conducts regular security workshops for system and network administrators from the government, defence, public sector and private sector. CERT-In has an important role to play in the overall cyber security efforts. While the Information Technology Act 2008 (ITA 2008) has made some headway in providing legal backing for the conduct of electronic surveillance and to bring cyber terrorists to book, it still needs to be backed up by a comprehensive set of rules focusing on the delivery of security on a national scale in cyberspace.

CERT-In should act as a fulcrum for formulating a National Cyber Security Strategy. Besides, it can act as a coordinating agency for national cyber intelligence and integrate the activities of cyber crime policing in different states. It can also enter into cyber crime prevention treaties with other countries to

ensure international cooperation against cyber terror. As a counter-intelligence strategy, it can counter-hack, plant its own intelligence gathering mechanisms where required, and defend the country from external aggression through cyberspace. Some similar roles and tasks as assigned to the US Department of Homeland Security could be examined in the Indian context and can be overseen by CERT-In. The organisation should be a single point of contact for the government's interaction with industry and other partners for 24/7 functions, including cyberspace analysis, warning, information sharing and major incident response[58].

The following is the relevant provision

Sec 70A : *(1) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.*

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

Sec 70B: *(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.*

(2) The Central Government shall provide the agency referred to in sub-section with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,—

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

---

[58] http://www.google.co.in/url?sa=t&rct=j&q=the%20indian%20computer%20emergency%20response%20team%20&source=web&cd=10&ved=0CGEQFjAJ&url=http%3A%2F%2Fwww.claws.in%2Fdownload.php%3Faction%3D1288165405MP_23__30.07.10.pdf&ei=95ddUPGuEc3orQfXioDACw&usg=AFQjCNGcbB8dXgrXIAJA9YWU57PL6kDDDQ.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service provides, intermediaries, data centres, body corporate and any other person.

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under subsection (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)."

Cyberspace provides a platform for innovation and prosperity and the means to improve general welfare around the world. But the broad reach of the loose and lightly regulated digital infrastructure poses great risks to nations, private enterprises and individuals. The Government of India has the responsibility of addressing these strategic vulnerabilities, to ensure that the country and its citizens, together with the larger community of nations, can realise the full potential of the information technology revolution. India's efforts towards the formulation of a National Cyber Security Strategy are not, so far, distinctly visible. With the enactment of ITA 2008, CERT-In has been provided with some teeth, in that it now has a statutory role to play. While the rules for such roles are being worked out, there is a fair amount of apprehension about some of the operating sections of the revised ITA 2008, especially those related to the protection of civil rights, rights to privacy and protection of propriety data.

Cyber security and personal privacy need not be opposing goals. Cyberspace security programmes must strengthen, not weaken, such protections. CERT-In must continue to meet regularly with privacy advocates to discuss cyber security and the implementation of ITA 2008.

In December 2009, Chinese hackers are believed to have attempted to penetrate India's most sensitive government offices, in the latest sign of rising tensions between the two rival Asian powers. M K Narayanan, India's former National Security Adviser, has stated that his office and other government departments were targeted on 15 December, the same date that several US companies reported cyber attacks from China. This was not the first instance of an attempt to hack into our computers, Narayanan told *The Times*. He said that the attack came in the form of an e-mail with a PDF attachment containing a Trojan, which allowed the hacker to access a computer remotely and download or delete files. The virus was detected and officials were told not to log on until it was eliminated. It is difficult to find the exact source of the virus but China seems to be the main suspect.

It seems well founded, Narayanan said, adding that India was cooperating with America and Britain to bolster its cyber defences. But both American and Indian officials believe that China is, at best, an Internet mischief-maker and, at worst, a potential cyber-adversary. US officials hope that tighter ties with India on Internet security issues can help make the networks of both countries stronger.

CHAPTER III - PROCEDURAL LAW RELATING TO CYBER CRIMES

Introduction

One of the important aspects of administration in modern democracies is the system of Criminal Justice. The need for the administration of Criminal Justice has been felt by humanity since the dawn of civilization. A number of institutions have been developed in course of time to administer justice to the people. In the operative part of the system of Criminal Justice there are four distinct components or constituent elements, namely; the Police, that is the investigative agency; the Prosecution, that is the agency to pursue a case in a court of law on behalf of the society; the courts, that is the Judiciary to try and decide about the guilt or innocence of a certain person and the Prison and correctional institutions.

3.1 Cyber Investigation:

The fundamental basis for Criminal Justice System is the law of the land. The very process of law in a democratic society ensures a measure of public sanction for law through the consent expressed by their elected representatives. The entire criminal justice system in our country therefore revolves round the Criminal Law enacted by the Union Parliament and the State Legislatures. After laws are made by the legislative institutions their enforcement is taken up by various agencies set up for the purpose by the Government. Police comes at this stage as the primary law enforcement agency available to the State. Enforcement by Police is primarily an exercise of taking due notice of the infraction of laws as soon as it occurs and ascertaining the connected facts thereof including the identity of the offender. This particular task in the system of Criminal Justice is known as ‘Investigation ‘.

According to judicial interpretation, investigation consists generally of the following steps:

1. Proceeding to the spot;
2. Ascertainment of the facts and circumstances of the cases;
3. Discovery and arrest of the suspected offender;
4. Collection of evidence relating to the commission of the offence which may consist of: (a) the examination of various persons (including the accused) and the reduction of the statements into writing, if the officer thinks fit; (b) the search of places or seizure of things considered necessary for the investigation are to be produced at the trial; and

5. Formation of the opinion as to whether on the material collected there is a case to place the accused before a Magistrate for trial, and if so taking the necessary steps for the same by the filing of a charge-sheet Under Section 173 of Code of Criminal Procedure.

No special procedure to conduct investigation, trial etc is provided in IT Act so the general procedure laid down in CRPC would apply with respect to investigation, charge sheet, trial, decision, sentencing and appeal of cyber crimes.

However Section 78 of the IT Act empowers police officers of the rank of Inspectors and above to investigate offences under the IT Act. Many states have set up dedicated cyber crime police stations to investigate offences under this Act. Thus, for example, the State of Karnataka and State of Andhra Pradesh has set up a special cyber crime police station responsible for investigating all offences under the IT Act with respect to the entire territory of Karnataka or AP.

3.2 Compoundable offences among Cyber Crimes:

Offences punishable with imprisonment of up to three years are compoundable by a competent court. However, repeat offenders cannot have their subsequent offences compounded. Additionally, offences which "affect the socio-economic conditions of the country" or those committed against a child under 18 years of age or against women cannot be compounded[59]. Compounding means complainant will compromise with the accused and withdraw his criminal complaint, which is normally not possible with any offence. Sec 324 of CRPC prescribes the procedure to compound the offence. Same procedure shall be followed for cyber offences as well.

3.3 Powers of Police Officers in Investigating Cyber Offence:

a. **Power to Confiscate**: Section 76 lays down the conditions under which documents or things which contain any information about the cyber crime or were used in committing the crime can be confiscated by police or investigating officer.

Some of the things which can be confiscated are: Hardware which can include any data-processing devices (such as central processing units, memory typewriters, "laptop" or "notebook"

[59] [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.
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 265C of Code of Criminal Procedures, 1973 shall apply.
[* Inserted vide Information Technology Amendment Act, 2008]

computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices).

b. **Power of Arrest**: Sec 80 of IT act empowers police with vast powers to search premises and arrest suspected accused. This provision empowers police to arrest by way of preventive action i.e., if police can suspect that a person is going to indulge in a cyber crime before he plunges into action police officer can arrest him. Another power given to police officer is arrest without warrant. All cyber crimes are recognized as cognizable offences. Sec 41 of Code of Criminal Procedure (CrPC) confers powers to arrest without a warrant in some grave and urgent situations. The rationale behind giving this power to police is to prevent accused from absconding. After arrest a police officer shall produce the arrestee in front of the nearest magistrate within 24 hours. A judge after perusing facts of the case will either send the person to police custody or judicial custody under as per section 164 of CrPC for further investigation and collection of facts. Unless the accused is a dangerous criminal police shall not hand cuff him. Arrest can be courted by word and if he surrenders to police there is no need to handcuff him. Sec 43 of CrPC gives power to go to extent of killing the accused if he is trying to evade arrest. But from the language of the section it is clear that it shall be the last resort. All these powers could be exercised by not only a police officer but according to the Act any officer appointed and authorized by Central or State Government can exercise with a condition that he or she shall handover the person or present him in from of the judicial magistrate without any delay.

c. **Search to arrest the accused**: Section 47 CrPC.: A Police officer is empowered to search anywhere in India outside his jurisdiction if necessary. In general they take the help of local police.

d. **Power to Search persons**: Section 156 CrPC. : Power to investigate cognizable offences. On mere suspicion that a person is involved in committing a crime or is potential to commit a crime police can arrest under this provision.

e. **Power to investigate non cognizable offences**: Section 155 CrPC. : In case of cognizable offence police can immediately go to the scene of offence arrest all suspected accused without a warrant, collect evidence and record statements of witnesses.

f. **Power to issue summons:** Section 91 CrPC. : Summon to produce documents. If a police officer has information that a person is in possession of some incriminating material such as floppy drives or pen drives etc. he can send summons to that person and ask him to produce the document or a

thing to the police officer for the purposes of investigation. Summons are written orders addressed to a person in whose possession the required document or a thing is available. Summons are generally served in person, and if he or she is not available they can be served to any other family member. In case if the house is locked summons would be pasted to a conspicuous portion of the house.

g. **Power to require attendance of witnesses**: Section 160 CrPC : As per this provision the Investigating Officer can summon persons who are acquainted with the facts of the case or can give some information about the offence could be summoned to come to the police station and give statements. These statements shall be recorded by Police officer and need not be signed by the maker of statement. These statements are called as 161 statements, which can be used during trial.

h. **Power to issue Search Warrant:** Section 93 CrPC : General provision as to search warrants. If a person doesn't respond to summons or refuses to receive summons the next coercive method available in criminal procedure is issuing of search warrant. In this process a police officer is entitles to enter any premises and search it and seize documents, which are useful for the investigation.

i. **Procedure for research**: Sec 100 of CrPC: Search: A police officer can enter the premises and has to prepare a seizure memo which contains a list of things seized in the said house. The search process shall be conducted in the presence of two respectable inhabitants of the same locality. They have to sign the seizure memo.

3.4 Bail in Cyber Crimes:

There are two classes of offences, bailable and non bailable recognized by Code of Criminal Procedure. Bailable offences are petty offences whereas non bailable offences are serious offences.

When an accused is arrested for the alleged commission of a cyber crime he can apply for bail. If the offence is bailable, court grants bail to him under sec 436 of CrPC. If the offence alleged is non-bailable, court grants bail Sec 437 or 439 of CrPC.

There is another classification on the basis of power of police to arrest the accused, i.e., cognizable and non cognizable offences, for a cognizable offence police officer can arrest the accused without a warrant and for a non cognizable offence he cannot do so without a warrant.

Information regarding the fact that whether a particular offence is bailable or not is available in the first schedule of CrPC. However, Section 77-B has been inserted under 2008 IT Amendment Act as per which the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Sec.77B: *"S-77B Offences with three years imprisonment to be cognizable*

(1) Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable."

The operation of 1st Schedule of the CrPC. has been made inapplicable by insertion of this section. However, with the insertion of this section, the offences can be categorized as under:

OFFENCE	Cognizable or non cognizable	Bailable or Non-bailable
The offence punishable with imprisonment less than 3 years	Non cognizable	Bailable
The offence punishable with imprisonment of three years	Cognizable	Bailable
The offence punishable with imprisonment of more than three years	Cognizable	Non-Bailable

Thus, as per the scheme of the newly inserted Section 77-B, the offences under the amendment bill can be classified as follows:

OFFENCE	Punishment	Cognizable or non cognizable	Bailable or Non-bailable
Section 65: Tampering with computer source documents	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs	Cognizable	Bailable
Section 66: Hacking with Computer system (if done dishonestly or fraudulently)	Imprisonment upto three years and/or Fine upto Rs. 5 Lakhs	-do-	-do-
Section 66A: Punishment for sending offensive	Imprisonment for a term which may extend to	-do-	-do-

messages through communication service, etc	three years and with fine		
Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto three years and/or Fine uptoRs. 1 Lakhs	-do-	-do-
Section 66C: Punishment for identity theft	Imprisonment upto three years and Fine upto Rs. 1 Lakhs	-do-	-do-
Section 66D: Punishment for cheating by personation by using computer resource	-do-	-do-	-do-
Section 66E: Punishment for violation of privacy	Imprisonment upto three years and/or Fine upto Rs. 2 Lakhs	-do-	-do-
Section 66F: Punishment for cyber terrorism	May extend to Life imprisonment	-do-	Non bailable
Section 67: Publishing obscene information in electronic form	**First Conviction:** Imprisonment upto three years and Fine upto Rs. 5 Lakhs **Second or subsequent Conviction** : Imprisonment upto five years and Fine upto Rs. 10 Lakhs	-do-	Bailable in case of first conviction only. Second or subsequent conviction shall be non bailable
Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form	**First Conviction:** Imprisonment upto Five years and Fine upto Rs. 10 Lakhs **Second or subsequent Conviction**:	-do-	Non-bailable in both first and second conviction

	Imprisonment upto Seven years and Fine upto Rs. 10 Lakhs		
Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	-do-	-do-	-do-
Section 67C (2): Deliberate Failure by the intermediary to preserve and retain information as specified by the Central Government	Imprisonment upto three years and Fine	-do-	Bailable
Section 68 (2): Deliberate Failure to comply with the order/direction of controller	Imprisonment for a term not exceeding two years or to fine not exceeding one lakh rupees or to both	Non cognizable	-do-
Section 69 (4): Failure to extend facilities to decrypt information to govt. notified agency	Imprisonment for a term which may extend to seven years and fine	Cognizable	Non bailable
Section 69A (3): Punishment for failure by the intermediary to comply with the order of the notified agency to block websites etc.	-do-	-do-	-do-
Section 69B (4): Deliberate failure by the intermediary to provide the notified agency with	Imprisonment for a term which may extend to three years and fine	Non Cognizable	Bailable

the technical assistance or online access to the computer resource			
Section 70: Unauthorized access to protected system directly or indirectly affects the facility of Critical Information Infrastructure	Imprisonment up to 10 years and fine	Cognizable	Non bailable
Section 72A: Punishment for Disclosure of information in breach of lawful contract	Imprisonment for a term upto three years or to a fine upto Rs. 5 Lakhs or to both	-do-	Bailable

3.5 Cyber Crime and Law of Evidence:

Cyber crimes are committed in a virtual space where the evidence would be intangible and doesn't exist in a permanent form. Collecting Cyber Evidence without any causing damage to it is a big task and requires good skill. The second difficulty in this process is getting the evidence admissible in court of law. Evidence act deals with all kinds of tangible evidence and it is not of much relevance to cyber crimes. To meet the requirement some amendments are made in Evidence Act.

Section 3 of the Evidence Act amended to take care of admissibility of Electronic Record as evidence along with the paper based records as part of documents, which can be produced before the court for inspection.

Presumptions in Law:

In any proceedings involving a secure electronic record, the court shall presume, unless contrary is proved, that the secure electronic record has not been altered since the specific point of time, to which the secure status relates

The law also presumes that in any proceedings, involving secure digital signature, the court shall presume, unless the contrary is proved, that the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record.[60]

By virtue of provision of Section 65A, the contents of electronic records may be proved in evidence by parties in accordance with provision of 65B.

Held- Sub section (1) of section 65b makes admissible as a document, paper print out of electronic records stored in optical or magnetic media produced by a computer subject to fulfillment of conditions specified in subsection 2 of Section 65B .

The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by person having lawful control over the period, and relates to the period over which the computer was regularly used.

a) Information was fed in the computer in the ordinary course of the activities of the person having lawful control over the computer.

b) The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy.

c) Information reproduced is such as is fed into computer in the ordinary course of activity.

d) Sec 65B of Indian Evidence Act governs the status of admissibility of electronic evidence, which was amended through IT act. However electronic evidence is fragile and one can easily manipulate it. Hence courts in India are hesitant to attach substantial weightage to cyber evidence. Courts generally insist on corroborative evidence before coming to a conclusion. Police department is not equipped properly to handle cyber evidence. Due to their ignorance valuable information is lost and as a result of which even though many crimes are being committed every day, very few cases only are going to courts for trial.

Sec 65: Admissibility of electronic records- *(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*

[60] *Societe Des products Nestle SA case 2006 (33) PTC 469 &State v MohdAfzal, 2003 (7) AD (Delhi)1*

admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall 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 electronic record 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 function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, 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 describing the 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 sub-section (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 purposes 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 its 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.

The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (s.67B) has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Unfortunately, the section covers everyone who performs the conducts outlined in the section, including minors. A slight awkwardness is created by the age of "children" being defined in the explanation to section 67B as older than the age of sexual consent. So a person who is capable of having sex legally may not record such activity (even for private purposes) until he or she turns eighteen.

Another problem is that the word "transmit" has only been defined for section 66E. The phrase "causes to be transmitted" is used in section 67, 67A, and 67B. That phrase, on the face of it, would include the recipient who initiates a transmission along with the person from whose server the data is sent. While in India, traditionally the person charged with obscenity is the person who produces and distributes the obscene material, and not the consumer of such material. This new amendment might prove to be a change in that position.

CHAPTER IV – INTERNET AND SOCIAL MEDIA

Introduction

Internet and Cyber Space has thrown open the debate on Freedom of Speech and Human Rights issue in a different dimension than those debates existing in the physical world prior to the net revolution. Internet today in essence poses challenges to the settled issues of what constitutes the limits of freedom of expression defined by the laws of the nations. By virtue of its worldwide concept, the conflict of a universal code for freedom of expression and the national concept of the limits of freedom are locked in horns. The speed and reach of the net will redefine the information flow and its impact on various issues of political, social and cultural impact. The debate on the regulation of such freedom and rights in the net revolves not merely on the regulation by law but also the dependence on technology related solutions to aid such regulation. The current developments include that of the 'filters' and 'label systems' for selective regulation and to minimize restriction of the net freedom.

The attempt to use these technological solutions is an attempt to solve the vexatious question of keeping certain segments away from a world where it is free for all in terms of age, space, culture and anonymity. Whether the technology will succeed and how far effective is yet to be assessed but the efforts are continuing. These solutions are of two kinds- the filters, which are hardware devices to be used by local and national level regulators on controlling the contents and the target audience. The second type of solution is appropriate labeling in the content of the Net for regulation. The Platform for Internet Content Selection developed by the Massachusetts Institute of Technology through the World Wide Web consortium aids labeling by first and third party and has been acknowledged and accepted as one fitting the industry standards. These labeling systems used along with appropriate filtering hardware could be effective of regulating the net for information which has to be kept away from select target groups like children and may not impose a blanket ban on access to all. However the debate is on who will decide about the issues, and how effective it will be?

4.1 Freedom of Expression in Internet

Freedom of expression and right to information has gained a universal recognition and is part of the various international declarations and conventions. Thomas Chocrane[61] in his article "Law of nations in Cyber Space" lists out the important declarations listed below:

[61] The Law of Nations in Cyberspace: Fashioning a Cause of Action for the Suppression of Human Rights Reports on the Internet by Thomas Cochrane. See <http://www.mttlr.org/html/volume_four.html/Cochrane.html>.

1. Article 19 of the Universal Declaration of Human Rights states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[62] Article 19 of the International Covenant on Civil and Political Rights contains a similar provision, guaranteeing

   > "the right to freedom of expression," including "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers . . . through any . . . media . . .", though this right may be limited as necessary to protect national security, public order, or public health or morals.[63]

2. The European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10, and the American Convention on Human Rights, Article 13, protect the freedom of expression with provisions substantially similar to those contained in the Universal Declaration and the ICCPR.[64] The European Convention, however, states that this right may be limited "in the interests of national security,... for the prevention of disorder or crime,... for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[65]

3. The American Convention also contains the caveat that the exercise of the right to freedom of expression may be limited as necessary for "the protection of national security, public order, or public health or morals."[66] Despite these qualifying provisions in the various human rights instruments, it is generally recognized that freedom of information is a superior right, not in competition with an equivalent right of the state to limit access to information for national security reasons.

4. In the well-known case of Sunday Times v. United Kingdom, the European Court of Human Rights explained that the decision maker in human rights litigation "is faced not with a choice between two conflicting principles but with a principle of freedom of expression that is subject to a number of exceptions which must be narrowly interpreted."[67]

---

[62] U.N. GENERAL ASSEMBLY, UNIVERSAL DECL. OF HUMAN RIGHTS, U.N. Doc. A/810, U.N. Sales No. 152.1.15 (1948) [hereinafter UNIVERSAL DECL. OF HUMAN RIGHTS].

[63] International Covenant on Civil and Political Rights, 1966 U.N. Jurid. Y.B. 178, U.N. Doc. ST/LEG/SER.C/4.

[64] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 312 U.N.T.S. 221, E.T.S. 5, as amended by Protocol No. 3, E.T.S. 45, Protocol No. 5, E.T.S. 55, and Protocol No. 8, E.T.S. 118, Article 10; American Convention on Human Rights, Nov. 22, 1969, 9 I.L.M. 673 (1970), Article 13.

[65] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 312 U.N.T.S. 221, E.T.S. 5, as amended by Protocol No. 3, E.T.S. 45, Protocol No. 5, E.T.S. 55, and Protocol No. 8, E.T.S. 118, Article 10.

[66] American Convention on Human Rights, Nov. 22, 1969, 9 I.L.M. 673 (1970), Article 13

[67] Sunday Times v. United Kingdom, 30 Eur. Ct. H.R. (ser. A) at 41 (1979). See also Observer and Guardian v. United Kingdom, 216 Eur. Ct. H.R. (ser. A) at 20 (1991)

5. All human rights regimes recognize a right to freedom of information or expression, although the scope of that right varies considerably. Freedom of information is probably least protected in the African Charter on Human and Peoples' Rights, which was adopted by Organization of African Unity in 1963, and has been adopted by virtually every African nation.[68]

6. Article 9 of the Charter protects freedom of information, declaring that "[e]very individual shall have the right to receive information" and that "[e]very individual shall have the right to express and disseminate his opinions within the law."[69] The African Charter is distinctive in that it proclaims duties as well as rights,[70] and these limitations could arguably limit the freedoms guaranteed in Article 9.

7. The African Charter, like the International Covenant on Civil and Political Rights, declares that individuals have responsibilities to their communities, but the Charter "is the first human rights treaty to include an enumeration of, to give forceful attention to, individual's duties." The duties of individuals are outlined in Articles 27, 28, and 29 of the African Charter, and Article 29 is particularly broad in reach.[71] Phrases such as "serve the national community," "not to compromise the security of the state," and "strengthen social and national solidarity" sound suspiciously like grounds on which a nation could seek to justify severe limitations on the right to freedom of information.

4.2 Indian Position

This assurance of protection to free thought and speech has been provided in more explicit terms under Article 19 (1) of the Constitution. It says:

19. Protection of certain rights regarding freedom of speech, etc.

(1) All citizens shall have the right-

---

[68] Human and People's Rights in Africa and The African Charter, Report of a Conference held in Nairobi from 2 to 4 December 1985 convened by the International Commission of Jurists, 93-94.

[69] African Charter on Human and People's Rights (Banjul Charter), June 27, 1981, 21 I.L.M. 59 (1981), art. 9.

[70] Burns Weston et al., Regional Human Rights Regimes: A Comparison and Appraisal, 20 Vand. J. Transnat'l L. 585, 608-14 (1987); Lees Flinterman & Evelyn Ankumah, The African Charter on Human and Peoples' Rights, in GUIDE TO INTERNATIONAL HUMAN RIGHTS PRACTICE 165-66 (H. Hannum 2d ed., 1992).

[71] Article 27. 1. Every individual shall have duties towards his family and society, the State and other legally recognised communities and the international community. 2. The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality, and common interest. Article 28. Every individual shall have the duty to respect and consider his fellow beings without discrimination, and to maintain relations aimed at promoting, safeguarding and reinforcing mutual respect and tolerance. Article 29. The individual shall also have the duty: 1. To preserve the harmonious development of the family and to work for the cohesion and respect of the family; to respect his parents at all times, to maintain them in case of need; 2. To serve this national community by placing his physical and intellectual abilities at its service; 3. Not to compromise the security of the State whose national or resident he is; 4. To preserve and strengthen social and national solidarity, particularly when the latter is threatened; 5. To preserve and strengthen the national independence and the territorial integrity of his country and to contribute to its defense in accordance with the law;... 8. To contribute to the best of his abilities, at all times and at all levels, to the promotion and achievement of African Unity. African Charter on Human and People's Rights (Banjul Charter), June 27, 1981, 21 I.L.M. 59 (1981), arts. 27-29.

(a) to freedom of speech and expression

(b) to assemble peaceably and without arms

(c) to form associations or unions;

(d) to move freely throughout the territory of India,

(e) to reside and settle in any part of the territory of India, and

(f) (it is omitted by the Constitution (Forty Fourth Amendment) Act, 1978, s. 8)

(g) topractise any profession, or to carry on any occupation, trade or business.

(2) Nothing in sub clause (a) of clause (1) shall effect the operation of any existing law, or prevent the State from making any law, in so far as such law imposed reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of sovereignty and integrity of India, the security of state, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

Article 19(2) was amended in 1951 and the State was allowed to make laws with the object of imposing reasonable restrictions on the exercise of the right conferred by Article 19(1) (a) in the interests of

1. Security of State,
2. Friendly relations with foreign states,
3. Public order,
4. Decency or morality
5. In relation to Contempt of court
6. Defamation
7. Incitement to an offence
8. Sovereignty and integrity of India (This ground is added in Article 19(2) by Constitution (Sixteenth Amendment) Act, 1963)

4.3 Public Order & Security of State:[72]

If an act has tendency to cause public disorder it would be valid ground under Article 19(2) to impose restrictions, even though it may not lead to breach of public order.

Supreme Court explained the meaning of the public order as that state of tranquility, which prevails amongst the members of a political society as a result of the internal regulations, enforced by the Government, which they have established.[73] The expression security of state refers to serious and aggravated form of public disorder and not ordinary law and order problem and public safety. The speeches and expressions, which encourage violent crimes, are related to security of State.[74]

4.4 Official Secrets:

Mere criticism of the Government action would not fall within the mischief of 'public order' and the same would be protected under Article 19(1)(a). The Supreme Court said referring to Section 124A of the IPC held that the activity would be rendered penal when it is intended to create disorder.[75] In the name of security, the Official Secrets Act of 1923 is still imposing severe restrictions on the freedom of expression. However, the governments in principle accepted to reduce the seriousness of this colonial legislation and provide for Right to Freedom of Information. The Official Secrets Act poses a major impediment in the process of providing right to information.

4.5 Incitement to an Offence:

The fundamental right of freedom of speech and expression ends when such incites the commission of violent crimes, which include attempts to insult the religious beliefs of any class. The aggravated forms of insult to religion which may clearly intended to disrupt public order are reasonable grounds based on which restrictions can be imposed on freedom of speech and expression. Promotion of disharmony among the classes during an election speech also can be restricted on the same ground. Seeking votes on the ground of candidates religious in a secular state is against the norms of decency and propriety of the society.[76] Thus Section 123(3) of Representation of People Act 1951, which imposes restriction on the exercise of right under Article 19(1) (a), is based on the support from Article 19(2) which includes 'decency' as a ground.

---

72 The following excerpts are taken from 'Media and Public Policy' Dr. Sridhar Acharyalu, Nalsarpro, p 71-80.
73 Ramesh Thapper v. State of Madras AIR 1950 SC 124
74 State of Bihar v. ShailaBala AIR 1952 SC 329
75 Kedarnath v. State of Bihar AIR 1962 SC 955
76 R.Y .Prabhoo v. P.K. Kunte AIR 1996 SC 1113

In ***Indulak K. Yagnik v. State of Maharashtra***[77] Section 3 of the Police (Incitement to Disaffection) Act 1922 was challenged as contrary to the fundamental right to freedom of expression. Bombay High Court held that the inducement of a police officer is punishable and thus the restriction on the free expression to prevent incitement to offences is valid under Article 19(2).

Similarly section 144 of Criminal Procedure Code which gives wide power to District Magistrates to impose restriction upon the fundamental rights of freedom of speech and assembly, is declared constitutional, in ***Babulal v. State of Maharasthra***[78] and ***State of Bihar v. K.K. Mishra.***[79]

4.6 Contempt of Court:

Contempt of Court has been recognised as a valid ground for imposing restrictions on the freedom of speech and expression. The Supreme Court in ***C. K. Dephtery v. D. P. Guptha***[80] held that the power of contempt administered by the Supreme Court under Article 129 is reasonable under Article 19(2). Section 228 of Indian Penal Code also makes the contempt of court punishable; Contempt of Courts Act 1952 also punishes it.

When former Chief Minister of Kerala, E.M.S. Namboodripad made various critical remarks against the judiciary at a press conference, he was questioned for contempt of court. He argued that the statement was protected under Article 19(1) (a). Rejecting the argument the Court held that while exercising the right of freedom of expression one should not commit contempt of court, and any comment, which could be contempt, is not protected by the Constitution.[81]

Supreme Court stated the object and content of this restriction in a recent case ***Narmada Bachao Andolon***[82] as follows: "No person is permitted to distort orders of the court and deliberately give a slant to its proceedings, which have the tendency to scandalize the court or bring it to ridicule. Hypersensitivity and peevishness have no place in judicial proceedings- vicious stultification and vulgar debunking cannot be permitted to pollute the stream of justice".

However, the newspapers and media channels have right to publish reports on the proceedings of the court, subject to the orders of the Court resolving the dispute. But if the Court orders not to publish a

---

77 AIR 1969 Bom 399
78 AIR 1961 SC 884
79 AIR 1971 SC 1667
80 AIR 1971 SC 1132
81 E. M. S. Namboodripad v. T. N. Nambiar AIR 1970 SC2015
82 AIR 1999 SC 3345

particular evidence of a witness, that is not an invalid order. Thus it cannot be said that press or TV channels have fundamental right to publish the court proceedings.

Causing Contempt of Court is not part of the freedom of press. In fact, contempt of court is a ground on which the press freedom can be restricted under Article19 (2). A news item stating that two sons of senior judge of the Supreme Court and two sons of the Chief Justice of India were favoured with the allotments of petrol outlets from the discretionary quota by the Petroleum Minister was published in some newspapers. The concerned Editors, Printers and Publishers admitted that the news item was false and was published inadvertently and without any malice to the judiciary. "The Sunday Tribune" in its issue dated March 10, 1996 published an item with a caption "Pumps for all". A similar item also was published in "Punjab Kesari". Contempt proceedings were taken up on the petition of K.T.S.Tulasi, and Additional Solicitor General besides some senior Advocates. Supreme Court held that the newspapers did not take even ordinary care to verify the truth of the allegations and did some disservice to the society by disseminating false information affecting the credibility of newspapers and causing embarrassment to the Supreme Court. The Court said that obviously this could not be regarded as something done in good faith. However, the Supreme Court accepted the apology tendered by the Journalists. The Court said: "he (senior Journalist) has no doubt, committed serious mistake but he has realised his mistake and expressed sincere repentance and has tendered unconditional apology for the same. He was present in the Court and virtually looked to be gloomy and felt repentant of what he had done. This sufferance in itself is sufficient punishment for him. He being a senior journalist and an aged person and, therefore, taking lenient view of the matter his apology was also accepted." The Court directed the contemners to publish in front page of their respective newspapers within a box their respective apologies specifically mentioning that the said news items were absolutely incorrect and false.[83] However, the Supreme Court in this judgment reiterated the importance of a vibrant free press in a democracy in the following words.

Freedom of Press has always been regarded as an essential pre-requisite of a Democratic form of Government. It has been regarded as a necessity for the mental health and the well being of a society. It is also considered necessary for the full development of the personality of the individual. It is said that without the freedom of press truth cannot be attained. The Freedom of the Press is regarded as "the mother of all other liberties" in a democratic society. A free and healthy Press is indispensable to the functioning of a true democracy. In a democratic set-up there has to be an active and intelligent participation of the people in all spheres and affairs of their community as well as the State. It is their right to be kept informed about current political, social, economic and cultural life as well as burning topics and important issues of the day in order to enable them to consider and form broad opinion about

[83] *In Re*: Harijai Singh and another, *In Re:* Vijay Kumar AIR 1997 Supreme Court 73

the same and the way in which they are being managed, tackled and administered by the Government and its functionaries.

4.7 Friendly Relations with Foreign States:

This is yet another ground justifying the restriction on the free speech. However state cannot prevent all the criticism of the foreign policy of the Government. The press should shun systematic diffusion of deliberately false or distorted reports, which undermines the friendly relations with foreign States.

The state has general power to impose restrictions on the free speech and expression provided such restrictions are reasonable. The standard of reasonableness has t be with reference to the subject matter of legislation and the import and the purpose for which such restrictions have been imposed and other prevailing circumstances. Restriction should not be arbitrary and excessive. There should be a balance between the freedom guaranteed and the community interest's protection of which necessitated the imposition of a restriction.

The Supreme Court held in ***Kharak Singh v State of Punjab***[84] that restriction couldn't be imposed through executive or departmental instructions. Reasonable restriction can be imposed by law enacted by the legislature.

4.8 Censorship of Books:

Mr. Ranjit D. Udeshi, a partner of a firm which owned the Happy Book Stall in Bombay was prosecuted and convicted under Section 292, Indian Penal Code for possession of an obscene book Lady Chatterley's Lover, which was unexpurgated edition. He appealed to Supreme Court, which upheld[85] the conviction. The court said that the opinions of literary or other experts were not relevant to the question of whether a publication is obscene. The court adopted the test of obscenity laid down by the Chief Justice Cockburn in ***Regina v Hicklin***[86], which is known as Hicklin test, where it was observed:

> The test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall…it is quite certain that it would suggest to the minds of the young of either sex, or even to persons of more advanced years, thoughts of a most impure and libidinous character.

---

84 AIR 1963 SC 1295
85 Rajit D. Udeshi v State of Maharasthra, AIR 1965 SC 881
86 [1968] 3 QB 360

4.9 Defamation:

Defamation is an injury to reputation of a person. It is both a crime and a tort. The law of civil defamation is not codified in India. However it provides for remedy in case a person's reputation is harmed without any justifiable reason. The law of criminal defamation is contained under Sections 499 and 500 of Indian Penal Code. If a person intentionally indulges in harming the reputation of another, he can be prosecuted for criminal wrong of defamation, which is a valid ground for imposing a restriction on freedom of speech and expression, under Article 19(2).

When Harbhajan Singh made scathing attack on the son of the Chief Minsiter Pratap Singh Kairon, he was prosecuted for defamation, in ***Harbhajan Singh v State of Punjab,***[87] the matter went up to Supreme Court. Mr. Singh accused the son of Chief Minister as the leader of smugglers and responsible for several crimes in the State. His conviction under defamation was set aside by the Supreme Court and because his statement was intended for the public good, the appellant was entitled to claim the protection of exception 9 to section 499 IPC.

Besides above restrictions, taxes and other trade related restrictions could be imposed on the press like any other ordinary individual is subjected to. The freedom of expression cannot protect a reporter or media person from being prosecuted for infringing the privileges of Parliament, which were guaranteed by a special provision Article 194(3) in the Constitution. However, there are restrictions possible on the exercise of such parliamentary privileges. If such an exercise of privilege violates the fundamental right to life and liberty without any legal basis and legal procedure, the Judiciary reserves the power to review such an assault.

The Supreme Court has set an agenda for development of law on the press freedom in Auto Shankar[88] case. It laid down certain foundations for making new principles of law on this subject at an appropriate time in future. It was in fact waiting for a right to case to arrive to study the impact of Article 19(1) (a) on the provisions of criminal defamation in Indian Penal Code, i.e., Sections 499 and 500. In principle the Supreme Court welcomed the wider interpretation of press freedom in *New York Times rule*[89] of US Supreme Court and *Derbyshire*[90] case in England. These judgments enhanced the scope of commenting on the public conduct of the public officials and reduced the scope of individuals occupying the public positions using the public office and public money for pursuing the

87 AIR 1966 SC 97
88 Supra note 6
89 Supra note 8
90 Supra note 7

actions for damages in defamation. While effectively providing for an individual civil remedy for defamation in favour of individuals there is need to review the continuance of the criminal defamation in present form.

Another gray area of development for law is the broadcast media. After holding that the state had no monopoly over the airwaves[91], the necessity to make statutes to regulate the electronic media by relieving it from the shackles of government controls. Exercise of press freedom in a vibrant democracy and its interpretation by active judiciary is a continuous process. New principles will evolve over a period of time in tune with the developing trends and needs of the democracy.

As the freedom of expression is vehemently being exercised by the media, especially electronic media, by arranging the meeting of the important personalities from different walks of life over a teleconference or video conference or on line conferences, and moving abroad for news coverage, the other rights under Article 19 are also essential to exercise the right guaranteed under Article 19(1) (a). The other rights are freedom of assembly, freedom of association, freedom of movement, right to property and freedom of trade and business.

Though the IT ACT has not specifically covered these issues, in Indian context 19(1) (a) and relevant restrictions will apply in the content of Internet.

[91] Supra note10

CHAPTER V: INTERNATIONAL LAW RELATING TO CYBER CRIME

Introduction

Cyberspace, as the fifth common space, after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyber threats. Peace, justice and security in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations. Critical information infrastructures of many governments and private industry have been targets by global cyber-attacks in the recent year.

The cyber-attacks on sensitive national information infrastructure are rapidly emerging as one of the most alarming international security threats, and could be considered as most serious cybercrime of global concern. Such attacks may have a great potential impact to the global economy, international security, and the critical information infrastructures of all nations.

5.1 United Nations

A treaty or a set of treaties at the United Nations level on cyber security and cybercrime should be a global proposal based on a potential for consensus. Serious crimes in cyberspace should be established under international law, whether or not they are punishable under the national law of a Party.

The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges on cyber security could be coordinated. In order to assist the ITU in developing strategic proposal, a global High-Level Experts Group (HLEG) was established in October 2007.

This global experts group of almost 100 persons from around the world delivered the Chairman's Report and the Global Strategic Report in 2008 with recommendations on cyber security and cybercrime legislations.

The United Nations Office on Drugs and Crime (UNODC) in Vienna, Austria organized the 12th of United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010, and the Congress made a recommendation in the Salvador Declaration Article 42. The Commission on Crime Prevention and Criminal Justice and other UN institutions made a follow-up, and the recommendation was adapted by the United Nations General Assembly in its resolution 65/230.

5.2 Global Working Groups

Three main Working Groups have been established in 2010 in order to make recommendations for potential new international legal responses to cybercrime. The United Nations has initiated a comprehensive study of the problem of cybercrime, recommended in the Salvador Declaration Article 42 to establish

> "*an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime"*

The Expert Group had its first meeting in Vienna in January, 2011.[92] The East West Institute (EWI)[93] established in June 2010 a Cybercrime Legal Working Group[94], in order to advance consideration of a treaty or a set of treaties on cyber security and cybercrime. The members are independent nongovernmental global experts on cyber security and cybercrime. The Working Group shall develop recommendations for potential new legal mechanisms on combatting cybercrime and cyber attacks, and *"develop a consensus-building set of proposals related to international law."* The group had its first workshop in Brussels in March, 2011, the second meeting just recently in Lausanne, and the next workshop held in March 2012. United States and the European Union have established a Working Group on Cyber security and Cybercrime at the EU-US Summit in November 2010.[95] The group is tasked with developing collaborative approaches to a wide range of cyber security and cybercrime issues. Among the efforts is, *"advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties."* The group had its first meeting in February 2011. EU has made additional remarks that large scale attacks, which are an emerging trend, are not fully covered in the Convention.[96]

---

92 See www.unodc.org.
93 See www.ewi.info.
94 This working group was established by a recommendation from Judge Stein Schjolberg, Norway, in a letter in May 27, 2010, to President EWI.
95 See www.europa.eu and MEMO/10/597.
96 Celia Malmstrom, Member of the EU Commission, in a speech in April 13, 2011.

5.3 EWI Cybercrime Legal Working Group Recommendations

The EWI Working Group will make proposals for non-partisan; objective non-political solutions that may promote collaboration and serve as a compromise for the global inter governmental organizations, and develop a consensus-building set of proposals related to an international criminal law for cyberspace.

- Establishing a Global Virtual Task Force for the investigation and Prosecution: A Global Virtual Task Force should be established, including law enforcements, INTERPOL, non-governmental organizations, key stakeholders in the global ICT industry and sector, financial service industry, academia, working in a partnership. A task force will be necessary for the prevention, detection, and reposes to the global cyber crimes and global cyber attacks in fast and effective investigative measures and arrests, having real-time access to global information in cyberspace.

- Establishing an International Criminal Court or Tribunal for Cyberspace (ICTC): Criminal prosecution based on international aw need an international criminal court or tribunal for any proceedings. The most serious cybercrimes of global concern could be considered in the list of crimes within the jurisdiction of the International Criminal Court (ICC). An alternative solution could be to establish an International Criminal Court or Tribunal for Cyberspace.

- Recommendations for a global treaty on cyber security issues: Security models for the Information and Communication Technology (ICT) in cyberspace must be developed on a global level, defining a global and national cyber security strategy. Technical and procedural measures, organizational structures, capacity building, and international cooperation are the most important issues that should be included in a global treaty.

- Blocking of child pornography websites: Additional recommendations for a treaty/framework on blocking of child pornography websites will be included. Blocking child pornography websites must be based on global and national solutions.

5.4 The International Criminal Court (ICC) and Cyber Crimes

The International Criminal Court (ICC)[97] was established at a conference in Rome in 1998 by 120 States. The Rome Statute of the International Criminal Court was adopted and it entered into force on July 1st, 2002. The Court is independent from the United Nations, but has historical, legal and operational ties with the institution. The relationship is governed by the Rome Statute and by other relationship

[97] www.icc-cpi.int

agreements. The International Criminal Court (ICC) is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court. The jurisdiction of the International Criminal Court is limited to States that becomes Parties to the Rome Statute, but then the States are obliged to cooperate fully in the investigation and prosecution. The Court would have no jurisdiction with regard to crimes committed on the territory of non-States Parties, or by their nationals or with regard to States Parties that have declared that they did not accept the Courts jurisdiction over certain specific crimes.

The International Criminal Court may have a role to play in the fight of massive and coordinated cyber-attacks against critical information infrastructures even today under the current jurisdiction in force. According to article 93, paragraph 10, the Court may upon request *" cooperate with and provide assistance to, a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court, or which constitutes a serious crime under the national law of the requesting State."*

Massive and coordinated cyber attacks against critical information infrastructures may qualify as a "serious crime".

If massive and co-ordinated global attacks in cyberspace are included in the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings. And the Prosecutor, which is an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on an exceptional basis. (Articles 18 and 53) In accordance with Article 18 on preliminary rulings regarding admissibility, the Prosecutor may *"seek authority from the Pre-Trial Chamber to pursue necessary investigative steps for the purpose of preserving evidence where there is a unique opportunity to obtain important evidence or there is a significant risk that such evidence may not be subsequently available."* Such an exceptional proceeding may very well be needed in investigations of massive and coordinated attacks against critical information infrastructures in cyberspace. It is also the Pre-Trial Chamber that later on eventually issues an arrest warrant.

An International Criminal Court or Tribunal is necessary Criminal investigation and prosecution based on international law, needs an international criminal court for any proceedings. An international criminal court has been called a missing link in the international legal system. Many most serious global

cyber-attacks will go unpunished without a criminal court or tribunal in action. When an International Criminal Court or Tribunal is established, then the principle of individual criminal accountability may globally be enforced. Anyone who commits any of the cybercrimes included in the international cybercrime law can be prosecuted by the court. This possibility may also be a cornerstone for the global cybercrime deterrence. An effective deterrence may be one of the primary goals for establishing a permanent court or tribunal. It will be a signal from the United Nations and the global community that global cyber-attacks are no longer tolerated. Provisions may be included in the list of crimes within the jurisdiction of the International Criminal Court (ICC) in The Hague. An alternative solution may be to establish a special International Criminal Court for Cyberspace as a subdivision of ICC in The Hague, since it may be a natural choice with all international courts inside, or in the urban area of this city. But as an alternative in Singapore, where the INTERPOL Global Complex (IGC) will be established and operational in 2013/14 especially on enhancing preparedness to effectively counter cybercrime.

5.5 International Criminal Tribunal for Cyberspace (ICTC):

An International Criminal Tribunal for Cyberspace must be a United Nations court of law, established through a Resolution by the Security Council in accordance with Chapter VII of the United Nations Charter.

The Tribunals authority could be prosecuting and sentencing the most serious cybercrimes and global cyber-attacks of global concern, and should have jurisdiction on issues as follows:

- Violations of a global treaty or set of treaties on cybercrime
- Massive and coordinated global cyber-attacks against critical information infrastructures The Tribunal must have concurrent jurisdiction in relation to national courts, but may claim primacy over national courts and take over investigations and proceeding at any stage. The Office of the Prosecutor should be operating independently of the Security Council, of any State, or any international organization, or of other organs of the Tribunal. Investigations are initiated by the Prosecutor at his/her own discretion on the basis of information received. Indictments must be confirmed by judges prior to becoming effective. The Rules of Procedure and Evidence must be based on, and in consistent with the Statute of the Tribunal. It should be guided by the Rules of Procedure and Evidence of other international criminal tribunals and courts, such as the ICC, the Tribunal for the former Yugoslavia (ICTY) and the Tribunal for Rwanda (ICTR).

An International Criminal Tribunal[98] for Cyberspace could be established in The Hague as the natural choice in 2013-2014. A possible International Criminal Tribunal for Cybercrime could as an alternative also be established in Singapore. The tribunal could be operational in time for the opening of Interpol Global Complex (IGC) in Singapore in 2013-14. It would open up a possibility of assistance and cooperation with an outstanding investigation institution. The Prosecutor may then be assisted very efficiently in the determination if a case is of sufficient gravity in order to justify further action by the Court. That would enable the global justice to promote the rule of law and ensure that the gravest international cybercrimes do not go unpunished. Tribunals have often been chosen since the formalities are more flexible when established by the United Nations Security Council. The latest Tribunal was decided on at a conference in the Peace Palace in The Hague on October 25, 2010, with the creation of PRIME Finance (Panel of Recognised International Markets Experts in Finance). It will serve as an International Financial Court established in The Hague.

A global virtual taskforce for the investigation and prosecution of the most serious cybercrimes of global concern A Global Virtual Taskforce established in operational partnerships with key stakeholders in the global information and communications technology, industry, financial service industry, non-governmental organizations, academia, and the global law enforcement through INTERPOL, will be necessary for the prevention and effectively combat global cybercrimes, especially for delivering fast time responses to cyber attacks. A basic platform must be the coordination and open sharing of knowledge, information and expertise between members of the taskforce, that may result in fast and effective investigative measures, arrests, convictions, and securing and preserving evidence in a way that ensures legal compliance across many jurisdictions. The main task for a Global Virtual Taskforce on cybercrime should therefore be to prevent, detect, and respond to cybercrime, by investigation and prosecution of the most serious cyber crimes and cyber attacks of global concern. A Taskforce could be overseen by a joint global Strategic Working Group. Establishing an INTERPOL Global Complex (IGC) in Singapore is a very important effort and development for the international law enforcement to effective counter cybercrime. A Global Virtual Taskforce for Cyberspace may also be seated in Singapore. Together, this cooperation may create the most efficient law enforcement support for all global cybercrimes.

The Prosecutor and the office of the Prosecutor shall be responsible for the investigation and prosecution of the most serious cybercrimes of global concern. The prosecutor must have the ability to act independently in a separate organ of the International Tribunal, and shall not seek or receive instructions from any Government or from any other source. The Prosecutors Office should have the power to seek the most efficient assistance in the investigation of cybercrimes.

[98] Tribunals have often been chosen since the formalities are more flexible when established by the UN Security Council. The latest Tribunal was decided on at a Conference in the Peace Palace Hague on October 25 2010.

5.6 INTERPOL

The Prosecutors Office may be assisted in the global investigation by two pillars: INTERPOL[99] has since the 1980s been the leading international police organization on knowledge about and global cooperation on computer crime and cybercrime investigation. The INTERPOL network enables police to share information on cybercrime, and to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections. It is very important that the investigators of cybercrimes may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have efficient cross border cooperation when cyber-attacks involve multiple jurisdictions.

The INTERPOL Global Complex (IGC) based in Singapore may go into full operation in 2013/14, and employ a staff of about 300 people. The Global Complex is an integral part of the INTERPOLs efforts to reinforce its operational platform and will focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime.

Models for a Virtual Taskforce

The Metropolitan Police Central e-crime Unit (PCeU) was established in UK in 2008, in partnership with the taskforce in the United Kingdom. The International Cyber Security Protection Alliance (ICSPA) is a business led global organisation. It is a non-for-profit organisation, established in 2011 to channel funding, expertise and assistance to law enforcement cybercrime units in both domestic and international markets. The National Cyber Investigative Joint Task Force (NCIJTF) chaired by the FBI in the United States.

5.7 The UN Charter and associated mechanisms:

The primary instrument in international law, to which the most number of nations are currently subscribed, is the Charter of the United Nations ["UN Charter"]. The use of force is specifically prohibited by UN Member states in Article 2(4), which proscribes the "use of force against the territorial integrity or political independence of any State."[100] The majority view is that this provision bars all use of force, except that used in lawful self-defense.[101] Also, the use of cyber force so as to adversely affect "military information capabilities, industrial and manufacturing information infrastructure, or technology-

[99] See www.interpol.int
[100] UN Charter, Article 2.
[101] Jackson Nyamuya Maogoto & Steven Freeland, "Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist", 41 *Int'l Law* (2007) 1104.

based civilian and government economic activities"[102] would violate Article 2(4) of the UN Charter only if such an attack were able to meet the unfortunately high standard of severity so as to impact the territorial integrity or political independence of the victim State.[103]

Furthermore, the UN Charter does not define terms of great relevance such as "acts of aggression," even though this terminology is used in Article 39 of the UN Charter. Article 39 merely states that the "the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression."[104]

"Acts of aggression", in fact, remained undefined for the most part, until the UN General Assembly Resolution 3314. This resolution attempted a comprehensive definition of "acts of aggression" under international law.[105] However, this effort was largely by way of enumerating different acts that would be considered acts of aggression[106], and obviously did not contemplate the unique nature of the problem posed by cyber force, considering that the resolution was passed as long back as in 1974. Article 1 of the resolution starts out the definition in the same terms as the UN Charter and defines aggression as "the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the UN, as set out in this Definition."

However, it could also be argued that the non-exhaustive list that was prepared by way of definition could easily create enough leeway to include state-sponsored CNAs within the definition of acts of aggression.[107]

While it would be convenient to rest the matter here, there are again two problems this course would pose- the first being that the question of individual accountability is altogether ignored, and, secondly, the adjudicatory mechanisms provided within the matrix of the UN Charter and associated mechanisms are suspect so far as efficiency and effectiveness is concerned.

The second concern brings us to a discussion of the adjudicatory body of the UN- the International Court of Justice. Article 33 of the UN Charter discusses dispute resolution, and clause (1) of this Article enjoins states to settle their disputes peacefully.[108] Failing this, the Security Council may "call upon the parties to settle their dispute", as per Article 33(2).[109] For one, this is problematic because it will come into play

---

[102] *Supra* n. 1, 186.
[103] *Supra* n. 19, 436.
[104] UN Charter, Article 39.
[105] GA Res. 3314 (XXIX), Annex, UN GAOR, 29th Session, UN Doc. A/9631 (Dec. 14, 1974).
[106] *Ibid,* Article 4.
[107] Noah Weisbord, "Conceptualizing Aggression", 20 *Duke J. Comp. & Int'l L.* 1 (2009), 37.
[108] UN Charter Article 33, para. 1.
[109] *Ibid.,* para. 2.

only when the disputed act is within the contemplation of the Security Council- and there is no evidence to say that cyber force is so included. Further, even if such acts are recognised by it, the probability of Security Council deciding to refer a case to the ICJ is quite low, especially considering that the permanent members of the Security Council are the States most likely to be involved in the future commission of acts of cyber force.

The advisory jurisdiction of the ICJ is also worth noting. The ICJ may give an advisory opinion on any legal question at the request of anybody authorized by, or in accordance with, the UN Charter.[110] It is undoubtedly true that a legal question is involved in determining whether a cyber-attack constitutes a use of force or an act of aggression. However, while states cannot prevent the issuance of an advisory opinion,[111] such opinion by their very nature are devoid of binding effect and are thus insufficient to meet the burden placed on us by CNAs.

5.8 *'Jus in bello'*: the law in war and the Geneva Protocols:

After the attempt to define aggression in the 1974 UNGA resolution, it was (understandably) felt that the existing law did not account for or adequately protect all of the person affected by such aggression, whether by being involved by it or by being targeted- directly or indirectly- by it. As a response, the Additional Protocol I to the Geneva Conventions was evolved in 1977[112] to address the individuals involved in committing acts of aggression. (The provisions as to protection of civilians, and the use of emblems etc. are sadly irrelevant to our purposes of fixing accountability as they contemplate acts such as humane internment, disclosure of the fact of being a member of armed forces etc.) The armed forces of a Party to a conflict were said to consist of "all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict."[113] This is useful in the sense that States are free to take punitive action against those who, acting under their command, violate rules of cyber warfare. Again, a problem arises in the fact that there is a lack of such specific and technical regulatory systems in most, if not all, nations and also that this continues to leave the question of non-state-sponsored aggression open. While cyber terrorism undoubtedly implies the existence of conflict, it cannot be brought within the Geneva Protocol mechanism purely because the actors involved can easily escape the definition of those

---

[110] Statute of the International Court of Justice, (June 26, 1945), Art. 65.

[111] *Interpretation of Peace Treaties with Bulgaria, Hungary, and Romania,* Advisory Opinion, 1950 I.C.J. 65, 71; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136, 46-47.

[112] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, (June 8, 1977), 1125 U.N.T.S. 3.

[113] *Ibid.*,Art. 43(1).

who are to be regulated in actions taken in combat.

5.9 The Articles on State Responsibility:

The Draft Articles on State Responsibility work on the principle that "Every internationally wrongful act of a State entails the international responsibility of that State."[114] The kinds of acts for which responsibility is attributed remain vague enough within these articles so as to include a cyber attack. It is also helpful that the States may be held responsible for both acts of commission and omission, as stated in Article 2: "There is an internationally wrongful act of a State when conduct consisting of an action or omission (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."[115] It is also a well-settled and non-context-specific customary principle of international law that states have a duty not to harm each other.[116] Thus, not restraining the acts of non-state actors carrying out a cyber-attack may also be considered an omission deserving of the attribution of responsibility to the State from which these attacks originated.

However, these Articles only establish principles that must be taken to an adjudicatory mechanism- the ICJ- where a determination will happen, and the efficacy of the ICJ has already been seen as limited. Furthermore, the articles completely ignore the individual accountability for cyber atrocities.

5.10 Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime entered into force in 2004 and seeks to lay down guidelines for all signatory states regarding the legislations to be adopted against cyber crimes, and aims to foster international cooperation in this endeavour.[117] While it does address the acts of non-state actors, it does not contemplate cyber warfare.

The crimes that are identified in this convention include: the damaging, deletion, deterioration, alteration or suppression of computer data;[118] serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;[119] and, the production, sale, procurement for use, import, distribution or otherwise making available a device designed or adapted for the purpose of committing any of the offenses just described against the

---

[114] "Draft Articles on Responsibility of States for Internationally Wrongful Acts", Report of the International Law Commission on the Work of its 53rd Sess, UNGAOR, 56th Sess, No 10 UN Doc A/56/10, Art 1.
[115] *Ibid.,* Art 2.
[116] *Corfu Channel Case*, *United Kingdom v Albania (Merits)*, [1949] ICJ Rep 4 at 2224.
[117] Council of Europe, CETS No 185, (2001) 41 ILM 282 and Additional Protocol not directly related to cyber attacks, CETS No 189, 2003.
[118] *Ibid.*, Art 4.
[119] *Id.*, Art 5.

confidentiality, integrity and availability of computer data and systems.[120]

Since illegal access, illegal interception, data and system interferences as well as misuse of devices are all sought to be covered under the Convention, this instrument could be used to address cyber espionage. One of the major pillars of this Convention is that of encouraging and facilitating international cooperation, in relation to investigations, proceedings and collection of evidence.[121]

This Convention is a path breaker and is commendable for its efforts to create and foster international cooperation on a large scale, and it could also be said that this is the beginning of a regime similar to that on climate change- where states recognise that they have a grave, shared concern and they need to act collectively to attack it.

5.11 The Indian scenario

India has recently realised the need for a comprehensive legal and policy framework to combat cyber attacks. However, the efforts as far as law is concerned, so far have been oriented towards attempting to include cyber crimes such as espionage and data theft within the ambit of terrorist acts.[122] In keeping with this, it is proposed to set up a National Counter Terrorism Centre to be an important pillar of security infrastructure.[123]

Furthermore, it has sadly been noted that India does not currently have a single treaty with any other nations regarding the extradition of cyber criminals, especially considering the vulnerability of our networks and our civilians to acts of cyber terrorism.[124] Like the infrastructure at so many other nations, India as well is dependent on digital measures for the administration of many services, an example being the Delhi Metro Rail Project.[125]

Until 2008, the Information Technology Act did not contemplate the criminalisation of the use of computers and the internet for large-scale devastation, but instead addressed acts such as hacking, distribution of obscene material and other e-commerce related crimes.

Awakened by the 26/11 Mumbai attacks as to the need to regulate the use of computer and internet technology, an amendment was introduced to the Information Technology Act ('IT Act') of 2000 to include 'cyber terrorism' as a crime under Section 66F. This need was noted upon realising the

---

120 *Id.*, Art. 6.
121 *Id.*, Art. 20.
122 "Cyber terrorism is bigger threat: Chidambaram on NCTC", *ANI*, (May 5th, 2012), available online at <http://in.news.yahoo.com/cyber-terrorism-bigger-threat-chidambaram-nctc-072458759.html>.
123 *Ibid.*
124 "Cyber crimes: India yet to sign treaty with other nations", PTI (October 5th, 2012), available online at <http://zeenews.india.com/news/nation/cyber-crimes-india-yet-to-sign-treaty-with-other-nations.html>.
125 *Ibid.*

extensive use of cyber communications and technology in the gaining of information as to physical targets, target populations and the place[126], with the end result being the devastating act of terrorism whose 4th anniversary is fast approaching.

In recognition of the potential abuse of the public server facilities provided by cyber cafes in India, it was proposed to enact the Information Technology guidelines for Cyber Cafes Rules in 2011, which would address the maintenance of log books by cyber cafes with complete details as to the identity of the users of the cafes.[127] This would work as a reactive measure, obviously, and one would also hope that it would deter potential miscreants from indulging in acts of cyber terrorism for fear of being easily identified.

India has thus prepared itself for domestic attacks from cyber criminals, but in the absence of meaningful agreements with other nations, this law will amount to nothing in the face of attacks that transcend national boundaries. Furthermore, this law does not equip India to deal with cyber warfare at a psychological level, such as what was observed in August 2012, where there was no use of unauthorised information but still the object of spreading terror was achieved.

Joint Working Group:

In October, 2012, the Indian government announced a plan to set up a permanent Joint Working Group (JWG) in association with the private sector to counter cyber attacks affecting economic and social development.[128] This plan includes the setting up of four pilot projects, entailing the setting up of a testing laboratory, a test audit, studying vulnerabilities of the critical information infrastructure and establishing a multi-disciplinary centre for excellence.[129] The temporary JWG envisaged the public-private partnership in the permanent JWG as dealing with an institutional framework, capacity building and developing standards and testing facilities for information technology products.[130]

It is hoped that the permanent JWG will make substantial changes to the vulnerability patterns of our government and military data. The capacity building measures are important in this regard. As has been noted earlier in the paper, India was identified as one of the countries with the potential to develop a software as sophisticated as the Flame virus, thereby establishing our capabilities so far as cyber/internet

---

126 Debarati Halder, "Information Technology Act and Cyber Terrorism: A Critical View", in CYBER CRIME AND DIGITAL DISORDER (Madhava Soma Sundaram * Syed Umarhathab eds., Manonmaniam Sundaranar University Publications Division: 2011), 81.

127 *Ibid.*,86.

128 "Cyber security panel high on India's agenda", IANS (October 16th, 2012), available online at <http://articles.timesofindia.indiatimes.com/2012-10-16/strategy/34497889_1_cyber-security-agencies-in-cyber-crime-cyber-attacks>.

129 *Ibid.*

130 *Id.*

technology is concerned. It would do us well to live up to this reputation in terms of defensive measures, and the proposed JWG, if fully operational, will certainly go a long way towards making this happen.

5.12 Draft on the National Cyber Security Policy:

In March 2011, the Department of Information Technology released a Discussion Draft on the National Cyber Security Policy, wherein it hearteningly identified the need for international cooperation in cyber security measures.[131] It has also identified some priorities for action for creating a secure cyber eco-system, which are as follows[132]:

a. Creation of necessary situational awareness regarding threats to ICT infrastructure for determination and implementation of suitable response;

b. Creation of a conducive legal environment in support of safe and secure cyber space, adequate trust & confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders and effective prosecution;

c. Protection of IT networks & gateways and critical communication & information infrastructure;

d. Putting in place 24 x 7 mechanism for cyber security emergency response & resolution and crisis management through effective predictive, preventive, protective, response and recovery actions;

e. Policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology & people) and incentives for compliance;

f. Indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes;

g. Creation of a culture of cyber security for responsible user behavior & actions;

h. Effective cyber crime prevention & prosecution actions;

i. Proactive preventive & reactive mitigation actions to reach out & neutralize the sources of trouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral & multi-lateral agreements with overseas CERTs, security agencies and security vendors etc.; and,

---

[131] Department of Information Technology, "Discussion Draft on the National Cyber Security Policy", (26th March, 2011), 5, Available online at <http://deity.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf>.

[132] *Ibid.*, at 6-7.

j. Protection of data while in process, handling, storage & transit and protection of sensitive personal information to create a necessary environment of trust.

After having made such identifications and issued statements as to the need to take immediate measures, however, all of the measures that have been taken between March 2011 and the present date are purely on a conceptual level.

5.13 DRAFT STATUTE OF THE INTERNATIONAL CRIMINAL TRIBUNAL FOR CYBERSPACE (ICTC)[133].

The United Nations Security Council, acting under Chapter VII of the Charter of the United Nations, has established the International Tribunal for the prosecution of the most serious violations of International Cybercrime Law, (hereinafter referred to as "the International Tribunal") and shall function in accordance with the provisions of the present Statute.

Article 1

Competence of the International Tribunal

The International Tribunal shall have the power to prosecute persons responsible for the most serious violations of international cybercrime law, in accordance with the provisions of the present Statute.

Article 2

Violations of the Global Treaty on Cybercrime

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

a) illegal access

b) illegal interception

c) data interference

d) system interference

e) misuse of devices

f) forgery

[133] Presented at ISPAC International conference on Cybercrime: Global Phenomenon and Its Challenges. Courmayeur, Italy 2011, by Judge Stein Schjolberg.

g) fraud

h) offences related to child pornography

Article 3

Violations of other provisions in the Global Treaty on Cybercrime

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law;

a) Spam

b) Identity theft

Article 4

Massive and coordinated global cyber-attacks against critical communications and information infrastructures

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law; whoever by destroying, damaging, or rendering unusable critical communications and information infrastructures, causes substantial and comprehensive disturbance to the national security, civil defence, public administration and services, public health or safety, or banking and financial services.

Article 5

Preparatory acts of provisions in the Global Treaty on Cybercrime.

The International Tribunal shall have the power to prosecute persons committing or ordering to be committed the most serious violations of international cybercrime law, namely the following acts committed willfully against computer systems, information systems, data, information or other property protected under the relevant international criminal law; the preparation of an information or communication technology tool or condition, that is especially suitable to commit a cybercrime.

Article 8

Jurisdiction

1. The jurisdiction of the Tribunal shall be limited to the most serious cybercrimes of concern to the international community as a whole. The Tribunal has jurisdiction in accordance with this Statute with respect to the crimes included in Articles 2-5.

2. The Tribunal shall exercise jurisdiction over additional cybercrimes according to future decisions of the Statute by the Security Council.

Article 9

Concurrent jurisdiction

The International Tribunal shall have primacy over national courts. At any stage of the procedure, the International Tribunal may formally request national courts to defer to the competence of the International Tribunal in accordance with the present Statute and Rules of Procedure and Evidence of the International Tribunal.

Article 10

Non-bis-in-idem

1. No person shall be tried before a national court for acts constituting serious violations of international cybercrime law committed under the present Statute, for which he or she has already been tried by the International Tribunal.

2. A person who has been tried by a national court for acts constituting serious violations of international cybercrime law may be subsequently tried by the International Tribunal only if:

   a) the act for which he or she was tried was characterized as an ordinary crime; or

   b) the national court proceedings were not impartial or independent, were designed to shield the accused from international responsibility, or the case was not diligently prosecuted.

3. In considering the penalty to be imposed on a person convicted of a crime under the present Statute, the International Tribunal shall take into account the extent to which any penalty imposed by a national court on the same person for the same act has already been served.

Article 11

Organization of the International Tribunal

The International Tribunal shall consist of the following organs:

a) the Chambers, comprising three Trial Chambers and an Appeals Chamber;

b) the Prosecutor; and

c) a Registry, serving both the Chambers and the Prosecutor.

Article 12

Composition of the Chambers

1. The Chambers shall be composed of a maximum of sixteen permanent independent judges, no two of whom may be nationals of the same State, and a maximum at any one time of twelve *ad litem* independent judges appointed in accordance with article 13 *ter*, paragraph 2, of the Statute, no two of whom may be nationals of the same State.

2. A maximum at any one time of three permanent judges and six *ad item* judges shall be members of each Trial Chamber. Each Trial Chamber to which *ad litem* judges are assigned may be divided into sections of three judges each, composed of both permanent and *ad litem*, except in the circumstances specified in paragraph 5 below. A section of a Trial Chamber shall have the same powers and responsibilities as a Trial Chamber under the Statute and shall render judgment in accordance with the same rules.

3. Seven of the permanent judges shall be members of the Appeals Chamber. The Appeals Chamber shall, for each appeal, be composed of five of its members.

4. A person who for the purposes of membership of the Chambers of the International Tribunal could be regarded as a national of more than one State shall be deemed to be a national of the State in which that person ordinarily exercises civil and political rights.

5. The Secretary-General may, at the request of the President of the International tribunal appoint, from among the *ad litem* judges elected in accordance with Article 13 *ter*, reserve judges to be present at each stage of a trial to which they have been appointed and to replace a judge if that judge is unable to continue sitting.

6. Without prejudice to paragraph 2 above, in the event that exceptional circumstances require for a permanent judge in a section of a Trial Chamber to be replaced resulting in a section solely

comprised of *ad item* judges, that section may continue to hear the case, notwithstanding that its composition no longer includes a permanent judge.

Article 13

Qualifications of judges

The permanent and *ad litem* judges shall be persons of high moral character, impartiality and integrity who possess the qualifications required in their respective countries for appointment to the highest judicial offices. In the overall composition of the Chambers and sections of the Trial Chambers, due account shall be taken of the experience of the judges in criminal law and international law.

Article 14

Officers and members of the Chambers

1. The permanent judges of the International Tribunal shall elect a President from amongst their number.
2. The President of the International Tribunal shall be a member of the Appeals Chamber and shall preside over its proceedings.
3. After consultation with the permanent judges of the International Tribunal, the President shall assign four of the permanent judges elected or appointed in accordance with article 13 *bis* of the Statute to the Appeals Chamber and nine to the Trial Chambers. Notwithstanding the provisions of article 12, paragraph 1, and article 12, paragraph 3, the President may assign to the Appeals Chamber up to four additional permanent judges serving in the Trial Chambers, on the completion of the cases to which each judge is assigned. The term of office of each judge redeployed to the Appeals Chamber shall be the same as the term of office of the judges serving in the Appeals Chamber.
4. After consultation with the permanent judges of the International Tribunal, the President shall assign such *ad litem* judges as may from time to time be appointed to serve in the International Tribunal to the Trial Chambers.
5. A judge shall serve only in the Chamber to which he or she was assigned.
6. The permanent judges of each Trial Chamber shall elect a President Judge from amongst their number, who shall oversee the work of the Trial Chamber as a whole.

Article 15

Rules of procedure and evidence

The judges of the International Tribunal shall adopt rules of procedure and evidence for the conduct of the pre-trial phase of the proceedings, trials and appeals, the admission of evidence, the protection of victims and witnesses and other appropriate matters.

Article 16

The Prosecutor

1. The Prosecutor shall be responsible for the investigation and prosecution of persons responsible for the most serious violations of international cybercrime law.
2. The prosecutor shall act independently as a separate organ of the International Tribunal. He or she shall not seek or receive instructions from any Government or from any other source.
3. The Office of the Prosecutor shall be composed of a Prosecutor and such other qualified staff as may be required.
4. The Prosecutor shall be appointed by the Security Council on nomination by the Secretary-General. He or she shall be of high moral character and possess the highest level of competence and experience in the conduct of investigations and prosecutions of criminal cases. The Prosecutor shall serve for a four-year term and be eligible for reappointment. The terms and conditions of service of the Prosecutor shall be those of an Under-Secretary- General of the United Nations.
5. The staff of the Office of the Prosecutor shall be appointed by the Secretary- General on the recommendation of the Prosecutor.

Article 17

The Registry

1. The Registry shall be responsible for the administration and serving of the International Tribunal.
2. The Registry shall consist of a Registrar and such other staff as may be required.
3. The Registrar shall be appointed by the Secretary-General after consultation with the President of the International Tribunal. He or she shall serve for a four-year term and be eligible for reappointment. The terms and conditions of service of the Registrar shall be those of an Assistant Secretary-General of the United Nations.
4. The staff of the Registry shall be appointed by the Secretary-General on the recommendation of the Registrar.

Article 18

Investigation and preparation of indictment

1. The Prosecutor shall initiate investigations ex-officio or on the basis of information obtained from any source, particularly from Governments, United Nations organs, intergovernmental and non-governmental organisations. The Prosecutor shall assess the information received or obtained and decide whether there is sufficient basis to proceed.
2. The Prosecutors Office shall have the power to collect evidence and to conduct all kinds of cyber investigation, and question suspects, victims and all other involved as parts and witnesses in the crime. In carrying out these tasks, the Prosecutor may, as appropriate, seek the assistance of the State authorities concerned.
3. The Prosecutors Office shall have the power to seek assistance in the investigation by INTERPOL and the INTERPOL Global Complex. The Prosecutors Office shall have the power to seek assistance in the investigation by a Global Virtual Taskforce established by key stakeholders in the global information and communications technology industry, financial service industry, non-governmental organisations, and the global law enforcement.
4. The Prosecutor may request a judge of the Trial Chamber, to issue such orders and warrants for the arrest, detention, surrender or transfer of persons, and any other orders as may be required for the conduct of the investigation or trial.
5. Upon determination that a *prima facie* case exists, The Prosecutor shall prepare an indictment containing a concise statement of the facts and the crime or crimes with which the accused is charged under the Statute. The indictment shall be transmitted to a judge of the Trial Chamber.

Article 19[134].

Review of the indictment

The judge of the Trial Chamber to whom the indictment has been transmitted shall review it. If satisfied that a *prima facie* case has been established by the Prosecutor, he shall confirm the indictment. If not so satisfied, the indictment shall be dismissed.

[134] Paper for East West Institute (EWI), Cyber Crime Legal Working Group, May 2011.

Article 20

Commencement and conduct of trial proceedings

1. The Trial Chambers shall ensure that a trial is fair and expeditious and that proceedings are conducted in accordance with the rules of procedure and evidence, with full respect for the rights of the accused and due regard for the protection of victims and witnesses.
2. A person against whom an indictment has been confirmed shall, pursuant to an order or an arrest warrant of the International Tribunal, be taken into custody, immediately informed of the charges against him and transferred to the International Tribunal.
3. The Trial Chamber shall read the indictment, satisfy itself that the rights of the accused are respected, confirm that the accused understands the indictment, and instruct the accused to enter a plea. The Trial Chamber shall then set the date for a trial.
4. The hearings shall be public unless the Trial Chamber decides to close the proceedings in accordance with its rules of procedure and evidence

Article 21

Rights of the accused

1. All persons shall be equal before the International Tribunal.
2. In the determination of charges against him, the accused shall be entitled to a fair and public hearing, subject to article 22 of the Statute.
3. The accused shall be presumed innocent until proved guilty according to the provisions of the present Statute.
4. In the determination of any charge against the accused pursuant to the present Statute, the accused shall be entitled to the following minimum guarantees, in full equality:
   (a) to be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him;
   (b) to have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;
   (c) to be tried without undue delay;
   (d) to be tried in his presence, and to defend himself in person or through legal assistance of his own choosing, if he does not have legal assistance, of this right; and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it;
   (e) to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(f) to have the free assistance of an interpreter if he cannot understand or speak the language used in the International Tribunal;

(g) not to be compelled to testify against himself or to confess guilt.

Article 22

Protection of victims and witnesses

The International Tribunal shall provide in its rules of procedure and evidence for the protection of victims and witnesses. Such protection measures shall include, but shall not be limited to, the conduct of camera proceedings and the protection of the victim`s identity.

Article 23

Judgment

1. The Trial Chambers shall pronounce judgments and impose sentences and penalties on persons convicted of serious violation of international cybercrime law.
2. The judgment shall be rendered by a majority of the judges of the Trial Chamber, and shall be delivered by the Trial Chamber in public. It shall be accompanied by a reasoned opinion in writing, to which separate or dissenting opinions may be appended.

Article 24

Penalties

1. The penalty imposed by the Trial Chamber shall be limited to imprisonment.
2. In imposing the sentences, the Trial Chambers should take into account such factors as the gravity of the offence and the individual circumstance of the convicted person.
3. In addition to imprisonment, the Trial Chambers may order the return of any property and proceeds acquired by criminal conduct, including by means of duress, to their rightful owners.

Article 25

Appellate proceedings

1. The Appeals Chamber shall hear appeals from persons convicted by the Trial Chambers or from the Prosecutor on the following grounds:
   (a) an error on a question of law invalidating the decision; or
   (b) an error of fact, which has occasioned a miscarriage of justice
2. The Appeals Chamber may affirm, reverse or revise the decisions taken by the Trial Chambers.

Article 26

Review proceedings

Where a new fact has been discovered which was not known at the time of the proceedings before the Trial Chambers or the Appeals Chamber and which could have been a decisive factor in reaching the decision, the convicted person or the Prosecutor may submit to the International Tribunal an application for review of the judgment.

Article 27

Enforcement of sentences

Imprisonment shall be served in a State designated by the International Tribunal from a list of States which have indicated to the Security Council their willingness to accept convicted persons. Such imprisonment shall be in accordance with the applicable law of the State concerned, subject to the supervision of the International Tribunal.

Article 28

Pardon or commutation of sentences

If, pursuant to the applicable law of the State in which the convicted person is imprisoned, he or she is eligible for pardon or commutation of sentence, the State concerned shall notify the International Tribunal accordingly. The President of the International Tribunal, in consultation with the judges, shall decide the matter on the basis of the interests of justice and the general principles of law..

Article 29

Co-operation and judicial assistance

1. States shall co-operate with the International Tribunal in the investigation and prosecution of persons accused of committing serious violations of international cybercrime law.
2. States shall comply without undue delay with any request for assistance or an order issued by a Trial Chamber, including, but not limited to:
   (a) the identification and locations of persons;
   (b) the taking of testimony and the production of evidence;
   (c) the service of documents;
   (d) the arrest or detention of persons;
   (e) the surrender or the transfer of the accused to the International Tribunal.

Article 30

The status, privileges and immunities of the International Tribunal

1. The Convention on the Privileges and Immunities of the United Nations of 13 February 1946 shall apply to the International Tribunal, the judges, the Prosecutor and his staff, and the Registrar and his staff.
2. The judges, the Prosecutor and the Registrar shall enjoy the privileges and immunities, exemptions and facilities accorded to diplomatic envoys, in accordance with international law.
3. The staff of the Prosecutor and of the Registrar shall enjoy the privileges and immunities accorded to officials of the United Nations under articles V and VII of the Convention referred to in paragraph 1 of this article.
4. Other persons, including the accused, required at the seat of the International Tribunal shall be accorded such treatment as is necessary for the proper functioning of the International Tribunal.

Article 31

Seat of the International Tribunal

The International Tribunal shall have its seat at The Hague, or at another location according to the Security Council decision.

Article 32

Expenses of the International Tribunal

The expenses of the International Tribunal shall be borne by the regular budget of the United Nations in accordance with Article 17 of the Charter of the United Nations.

Article 33

Working languages

The working languages of the International Tribunal shall be English and French.

Article 34

Annual report

The President of the International Tribunal shall submit an annual report of the International Tribunal to the Security Council and to the General Assembly.

CHAPTER VI: EMERGING AND CONTEMPORARY ISSUES IN CYBER SPACE

This chapter introduces the student to the new concepts of Data Protection along with technology concepts such as Quantum Computing, Artificial Intelligence, IoT, Big data etc.

This chapter is divided in to three parts. Part A discusses the concept of Data Protection and its relevance to Privacy Protection. Part B discusses some emerging technology developments which pose significant challenge to Privacy Protection. Part C discusses three major Data Protection Regulations that are relevant for Indian Companies namely HIPAA, GDPR and PDPA 2018 (Proposed), along with the framework for compliance under personal Data Protection Standard of India (PDPSI).

It may be noted that Section 43A which was relevant for Privacy Protection through Data Protection will be replaced by the new Act presently flagged as PDPA 2018. This will make PDPA 2018 as the next generation Cyber Law which will become an essential knowledge base for all Cyber Law Students.

As an emerging field of Techno Legal nature, cyber jurisprudence in these matters is still under development. I therefore encourage the students to look at the challenges of data protection without being unduly constrained by some of the Judicial Pronouncements of the past. A fresh look with a fresh mind is required to make Data Protection Laws clear.

Part A: Concept of Data Protection

"Data Protection" has become one of the most talked about subjects in the field of IT in the recent days.
The Concept of "Data Protection" emerges from two distinct points of Origin. First is of technical origin where "Data" is an asset in electronic form which needs to be protected like any other asset by its beneficial owner and/or custodian. The second is of Legal origin where "Data Protection" is a means of protecting "Privacy" of an individual because Privacy is a human right that is respected and protected in every democratic society.
Some of the Data Protection laws originate from the concept of protecting "Data" because it is an asset with value. Some of the data protection laws originate from the concept of protecting Privacy of an individual. We need to understand this distinction to avoid perceived conflicts of law.
For example, in India, we have Information Technology Act 2000 as modified in 2008 (ITA2000/8) which is meant to protect "Data". In other words, it defines the responsibility of persons in possession of

data to ensure that data is not unauthorizedly accessed, modified, deleted or otherwise injured. It prescribes penalties and punishments for violation of the provisions and also indicates the security prescriptions/due diligence which would make a person not liable in case some thing goes wrong. Parts of the amendments of 2008 to ITA 2000 was to specifically incorporate Privacy Protection into ITA 2000 without any ambiguity.

On the contrary, India is now considering passing a new specific law which may be called "Personal Data Protection Act" which is an approach to protecting the "Privacy" of an individual as a constitutional right. For this purpose, a bill was introduced in the parliament titled Personal Data Protection Act 2018 (PDPA 2018) in August 2018. This draft Bill may get reintroduced and passed in the next Parliament and would be a key legislation that defines the Data Protection regime in the country.

Some of the issues of apparent conflict in the domain of Data Protection arise because of the different objectives with which technologists approach Data Protection as against how a human rights activist approaches Data Protection. We need to first get our clarity in this respect.

I. "Data Protection" as "Protection of Data":

For a long time, it has been recognized that "Data" is an "Asset" for an organization. Some data is acquired at a cost and some attain value during the process of the operations of an organization both because of the money invested in its acquisition and development into a useful set of information.

Data consists of "Core Data" and "Meta Data". Meta Data is "Data about Data" and keeps accumulating as the "Data" is being used or processed in the ordinary course of its use.

Some Data refers to an "Individual". Individually identifiable data is referred to as "Personal Data". A part of the "Personal Data" is also identified as "Sensitive Personal Data" depending on the type of information about an individual that it may contain. Sensitive personal data is a sub set of Personal data and Personal Data is a subset of "Data".

Some personal data may refer to an individual who is recognized as a "Minor" with some special status in law and hence personal data of a minor may have a different sensitivity parameters attached to it. Law recognizes that a minor is represented by his "Guardians" and hence the right to manage the personal information of a minor may vest in a person other than the individual himself if he is recognized as a "Guardian". In such cases, the personal data of the guardian also becomes attached to the personal data of a minor and acquires sensitivity higher than the personal data of an adult per-se. In addressing the "Data Protection" related to minor's personal data, there is an overlap of the law of minority with the law related to "Data" and adds a dimension of its own.

In an organization, “Data” which is not “Personal” may be called “Corporate Data”. Corporate Data may be financial data, Marketing data, Operational data or Business data. HR data which is “Corporate Data” by nature may contain elements of “Personal Data” of employees. Similarly, Business data such as invoices may contain Customer data such as the name and address and even the PAN number of an individual which are also considered as Personal Information.

Thus, part of corporate data may be personal data and there could be an incidence of the personal data protection laws on the activities of collection, processing, storing and transmission of data which otherwise appear as corporate data.

Data by nature is “Dynamic”. With each operation, data changes its nature subtly by modification of “Meta Data”. “Aggregation” of data from different sources adds value during the processing. “Aggregation” can be an aggregation of data of one individual from different sources or aggregation of data of more than one individual. Both changes the nature of “Raw Data” and makes “Data” dynamic.

It is in this context that “Big Data” poses a challenge of its own on the Data Protection legislation.

II. Evolution of Data Protection Laws:

Recognizing “Data” as an “Asset”, most countries created laws for “Data Protection” in the first place as “Laws related to keeping information secure”. These took the shape of “Cyber Crime Laws” under which if Data is misused for purposes for which it was not meant, the action would be recognized as a contravention of law leading to civil and criminal punishments of different nature. Such laws did not distinguish between “Corporate Data” and “Personal Data” and the responsibilities and liabilities were defined as common prescriptions across all kinds of data.

When India enacted Information Technology Act 2000 it was meant to promote E Commerce and prevent Cyber Crimes. Hence the law was applicable to all kinds of data whether it was personal or corporate.

However, the increasing concern for “Protection of Privacy” when the society was passing through the “Digitization Phase” slowly brought more focus on the need to protect “Personal Information in electronic form”. Gradually this came to be recognized as “Data Protection”.

The first attempt of the law makers was to incorporate the requirements of protecting “Privacy” of an individual into the Data protection legislation by making some changes. An example could be seen in the amendments brought to ITA 2000 in 2008 when Sections 72A, 43A were introduced in the legislation

along with some consequential amendments such as Section 67C (Data Retention) and Sections 69,69A,69B,70B etc (Providing rights to different agencies to override the Privacy protection rights).

But the demand for a separate law for protecting Privacy did not recede and it is now surfacing in the form of PDPA 2018.

Today when industry professionals speak of "Data Protection", they are perhaps talking of "Personal Data Protection" and not the "Personal cum Corporate Data Protection".

The first clarification that the student of Data protection should develop is therefore to distinguish the scope of "Data Protection" that we discuss in this chapter. For most part of our discussion, we will be discussing "Personal Data Protection" and not "Total Data Protection". To distinguish the two, we normally use the terminology of "Information Security" for "Total Data Protection".

Thus in our discussion, "Information Security" more often refers to the protection of both corporate and personal data while "Data Protection" refers to the protection of personal data.

III. Data and Human Experience of Data

"Data" and "Information" are not inherently different. Both refer to a sequence of binary characters. It is important to also take note that both "Data" as well as "Information" refer to what a human being perceives when he looks into a sequence of binary data through a device which interprets that sequence of data.

Every human experience of "Data" is an interpretation rendered by a "Device" which more often we call as a "Computer". The experience can be as a "readable Text", audible "Sound" or an audio visual. In future we will have touch and smell sensors rendering the sensation of touch and smell through binary data interpreted by appropriate computing devices. Even the sense of "taste" is a kind of message conveyed by the taste buds in the tongue to the brain of a human and can be simulated by directly sending electro magnetic messages to the brain.

Thus all the five senses of a human being namely what a person sees, hears, what speaks/tastes, smells or senses by touch can all be rendered through binary expressions provided we have the appropriate devices that can interpret them.

An audio file read through a text rendering device will throw up junk and vice versa. Hence the human experience of data is dependent on the intermediary device that interprets the data and converts it into a

human experience of sight, sound, taste, smell or touch. If there is a mismatch of the type of data and the type of the device that reads the data, the human experience will not be the consistent or predictable. The Data Protection laws need to understand these challenges and address them in the legislation. Considering the complexities involved, the law as is written may not be always adequate and needs to be interpreted by Cyber Jurisprudents. In making such interpretations, we need to keep in mind the power and the limitations of technology and needs for a legal structure to provide comfort to the humans.

It is in this context that Internet of Things (IoT) provides a challenge of its own when it comes to "Data Security".

IV. Nature of Binary Data

Looking at "Binary Data" itself, it resides in the state of some "Data Holding Device". In the most common form, we may have a hard disk where there are millions of data spaces each of which can either have magnetism or not.

Data can be rendered in other forms as well. For example, there can be series of light bulbs some in on condition and some in off condition. There can also be a sequence of sound that comes as "Tap" or "No Tap" at regular intervals. There can also be a surface which may have plain surface and depressions in regular intervals. All these can be used to represent data in binary form where one state of the data holding platform represents zero and the other one.

Whatever be the manner in which a "Zero" and "One" is rendered, the sequence is a "Binary" expression and the device that can read the specific states can convert it into a human experience.

Thus the essence of our discussion on Data Protection is how that sequence of binary states of a platform which is recognized as "Data" is "Protected".

This requires also a definition of what is "Protection".

V. The CIA Principle of Data Protection

"Preservation of the Confidentiality, Integrity and Availability" is called the CIA principle of Information Security and is considered the basic definition of Information Security.

Over the years, this CIA principle has been extended into two more concepts namely "Authentication" and "Non Repudiation".

The “Information Assurance” approach to Information Security therefore recognizes Information Security as

> “Preservation of Confidentiality, Integrity, Availability, Authentication and Non Repudiation of Information/Data”.

“Confidentiality” essentially means that data/information is meant to be accessed only by persons who have a need to access for a stated organizational objective.

“Integrity” essentially means that data/information remains in the same state unless it is modified by an authorized person to create a modified version.

“Availability” essentially means that data would be available for the organizational requirements when needed without unauthorized interruptions.

“Authentication” essentially means that the data content and integrity should be accounted to some reliable source who is the owner of the data.

“Non Repudiation” essentially means that the content, integrity and ownership of data should be recognized under law and defendable in a Court.

When all these five parameters are present in an organization we can say that “Data is Protected”. It is the objective of Data Protection Managers to ensure that through appropriate tools these five parameters of data protection objectives are achieved. Such tools are often referred to as “Controls”.

These Controls may be technical in nature and may include software, hardware, physical locks, guards etc. It may also be of legal nature in the form of policies and procedures written down and enforced. It can also be connected with human behavioural aspects including creation of awareness, trainings, modification of behavioural patterns etc.

This 5 parameter security approach in the three dimensions of Technology, Law and behavioural Science is referred to as the “Three Dimensional Approach to Information Security Management” or “Total Information Assurance”. [i]

Prioritization of Information Assurance Principles:

"Security is as strong as the weakest link" and hence if there are five principles of information security, and even if one of them is absent, then information is not secure.
However, in practice, "Achieving Information/Data Security" is a "Journey" and it takes efforts to reach different milestones in an organization over a period of time. Hence managements need to have some kind of prioritization of information security implementation.

One of the ways in which this prioritization options are determined by an organization while implementing information security is through the "Pyramid Model" where the above five principles of Information Security is targeted for achievement one after the other.

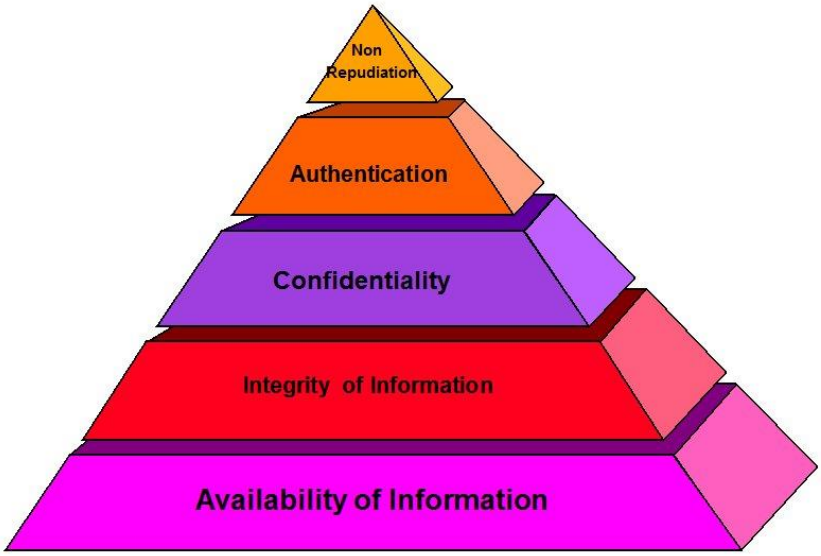


Figure 1: Pyramid Model of IS implementation

According to this Pyramid model of prioritization, an organization starts its Information/Data Security implementation with "Availability" and moves through "Integrity", "Confidentiality", "Authentication" and "Non Repudiation" in that order.

VI. Pentagon Model of Data Security:

While this "Pyramid Model" is a good representation to define the "Implementation" of an Information Security program, in order to define "Data Security", it is preferable to adopt a **"Closed Polygon model"** where several goals need to be achieved together before declaring the achievement of "Data Protection".

This "Polygon Model" approach has been adopted in the **"Personal Data Protection Standard of India"** (PDPSI)[ii] and represented in the diagram below. This model is referred to as the "Pentagon Model of Personal Data Protection"

In this model, the recognized elements to be achieved for Data Protection are

1. Classification of Personal Data for protection
2. Assignment of Responsibilities for Data Protection
3. Technical Controls for Managing protection of Personal Data
4. Compliance of Data Protection Regulations
5. Building a Culture of compliance

These five elements form a "Pentagon" and when achieved, creates the secure framework for "Data Protection".

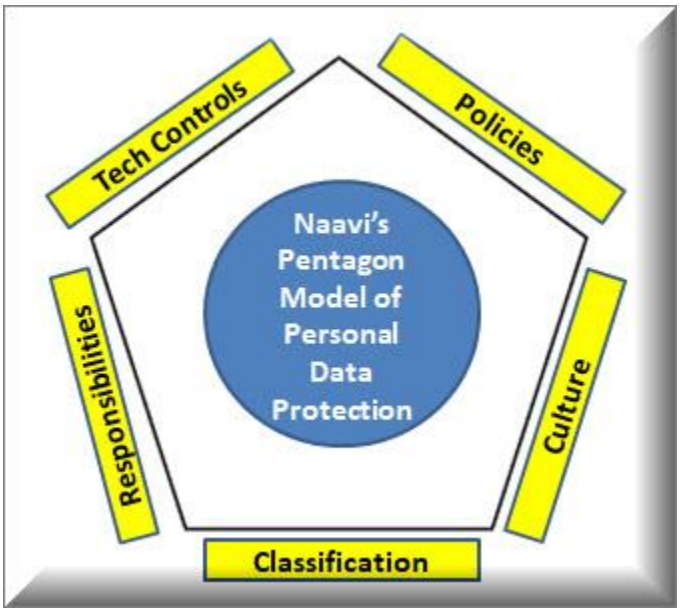


Figure 2: Pentagon Model of Personal Data Protection

The above concepts are explained in detail in the subsequent part of this lesson as part of the Personal Data Protection Standard of India. (PDPSI).

VII. “Data Protection” as “Protection of Privacy”:

While protecting data that contains personal information is part of the assets of an organization and it needs to be protected just as any other data, there is a separate demand that “Personal Data” is inherently the property of the individual to whom it belongs to whom we some times call as the “Data Subject” and he alone should have the right of its disclosure and use. Any use of such data without the knowledge of and permission of the data subject is considered as an “Infringement of the Rights of Privacy” of the data subject which is sought to be guaranteed as an essential human right in any democratic society.

This approach to “Personal Data Protection” is otherwise also referred to as “Information Privacy”.

In USA and EU countries, Privacy had been recognized as a fundamental right of the citizen for a long time. The culture of those countries imbibed the “Privacy” as a fundamental attitude of the people. So, when the society moved from the paper based activities to electronic document based activities, the country smoothly adopted to the concept of “Information Privacy”. The right of privacy of a citizen when his personal data is collected, processed, stored and disclosed were well defined in the paper world and got extended to the electronic world of “Information Privacy” without much of a need for re-adjustment of the society.

The situation in India was not exactly similar. Indian culture based in the vedic traditions always considered “spreading of knowledge” as a basic duty of a citizen and hence whether it was scientific knowledge or personal information, the culture of the people was against secretive dealings. Both the IPR as well as the Privacy Right were concepts imported from the western world and hence do not constitute the inherent nature of the people.

For example, in the Indian culture, not enquiring about the neighbour’s health or salary and not visiting him when he is ill is considered a disrespect. On the other hand in the Western Culture, health and financial information is so sacrosanct that even the parents and spouses are not privy to such information.

There is no doubt that just as we have adopted the global culture in many other respects, Indians also have adopted and are trying to adopt to the western culture and have accepted that “Privacy” is an important human right to be respected and protected by law.

However this culture of "Privacy" is more acquired and imposed than an inherent attitude and hence in an organizational environment, it becomes necessary to drive attitudinal changes and behavioral adjustments to bring about a globally acceptable standard of Privacy compliance.

Legally speaking, Indian constitution did not specifically mention "Privacy Right" as a fundamental right.

Article 21 of our constitution reads

> **Protection of life and personal liberty:** "No person shall be deprived of his life or personal liberty except according to a procedure established by law."

The "Right to Life" is a "Right to lead a dignified human life". Right to "Personal Liberty" includes "Right to be Left Alone".

Under these thoughts, the Supreme Court has in various decisions had held that Article 21 guarantees the Right to Privacy of an Indian Citizen.

In Maneka Gandhi Vs Union of India[135], the Supreme Court said that the "Right to live is not merely a physical right but includes within its ambit the right to live with human dignity".

Speaking of "Personal Liberty", in the Kharak Singh Vs State of UP[136], Article 19 of the Constitution was invoked.

The seven member bench in the Kharak Singh case held that though the Constitution contained no explicit guarantee of a "right to privacy", it read the right to personal liberty expansively to include a right to dignity. It held that "an unauthorized intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man -an ultimate essential of ordered liberty, if not of the very concept of civilization".

Justice Subbarao in the same judgement went further to express his opinion that

> "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements but also free from encroachments on his private life. It is true our Constitution does

[135] (AIR 2006 SC 1367)
[136] (AIR 1963 SC 1295)

not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his 'castle'; it is his rampart against encroachment on his personal liberty".

Further in R.Rajagopalan v State of Tamil Nadu[137] the Supreme Court stated

> "the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent – whether truthful or otherwise and whether laudatory or critical…...If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages."

With these judgements, for all practical purposes, Privacy was recognized as a fundamental right in India and the law was being interpreted accordingly.

However, recently in the context of the widespread opposition to the "Aadhaar", several references were made to the Supreme Court on the ground that Aadhaar violated Privacy and therefore should be scrapped. While discussion on this matter was taken up in the Supreme Court, a reference was made by the Attorney General that in the M P Sharma Vs Satish Chandra[138], it had been suggested that "Privacy" is not a "Fundamental Right" and had stated

> "fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right by some process of strained construction".

The decision of the M P Singh case was by a bench of 8 judges and hence carried a high constitutional weight.

However in the light of the strong opposition to Aadhaar, the Supreme Court considered that it was time to review the M P Singh verdict and therefore constituted a bench of 9 judges headed by the CJI Dipak

[137] (1995 AIR 264, 1994 SCC (6) 632
[138] (1954 AIR 300, 1954 SCR 1077)

Mishra and went into the analysis of whether "Right to Privacy" is a fundamental Right in India. This judgement which is often referred to as the "K S Puttaswamy Judgement" [iii] held

> (i) The decision in M P Sharma which holds that the right to privacy is not protected by the Constitution stands over-ruled;
>
> (ii) The decision in Kharak Singh to the extent that it holds that the right to privacy is not protected by the Constitution stands over-ruled;
>
> (iii) The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.
>
> (iv) Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law.

It is therefore an unambiguous situation in India that "Right to Privacy" is a fundamental right of the citizen protected by the Constitution as part of Article 21.

However, like every other fundamental right, Right to Privacy is subject to the power of the Government to impose "Reasonable Restrictions".

Article 19(2) indicates the description of the "Reasonable Restrictions"

It states

> "Nothing in sub clause (a) of clause (1) (Ed: Which is considered as applicable to all Fundamental Rights) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in 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"

Invoking of the Reasonable Restrictions clause require

1. There must be a law in existence to justify an encroachment of privacy.

2. There should be a requirement of a need in terms of a legitimate state aim
3. The means adopted by the legislature should be proportional to the object and needs sought to be fulfilled by the law.

The controversy surrounding the legality of Aadhaar was resolved by the Supreme Court under the above principles using the Aadhaar Act as the legislation and the power to impose reasonable restrictions on Privacy for a State aim.

However the Puttaswamy Judgement left an indelible impact on the issue of "Privacy" and reflects in other legislations including the Data Protection regulation that is coming up.

Despite a judgement that ran into 547 pages, the Puttaswamy Judgement did not define "Privacy". Different judges in their individual judgements expressed their own thoughts about "What Constitutes the Privacy Right of an Individual" but the portion of the signed judgement did not contain a gist of these thoughts which could be used as a "Definition".

Justice Chelmeshwar in his part of the judgement stated

- " **Whether it is possible to arrive at a coherent, integrated and structured statement explaining the right of privacy is a question that has been troubling scholars and judges in various jurisdictions for decades."** And

- "**In my opinion, there is no need to resolve all definitional concerns at an abstract level to understand the nature of the right to privacy….Definitional uncertainty is no reason to not recognize the existence of the right of privacy….**".

He then concludes that "**for the purpose of this case, it is sufficient to go by the understanding that the right to privacy consists of three facets i.e. repose, sanctuary and intimate decision. Each of these facets is so essential for the liberty of human beings".**

These three facets "repose", "Sanctuary" and Intimate Decision" are picked from academic concepts postulated by a US author Bostwick.

"Repose" refers to freedom from unwarranted stimuli, "sanctuary" to protection against intrusive observation, and "intimate decision" to autonomy with respect to the most personal life choices. All these are covered under the concept of Privacy being "Right to be Left Alone".

Unfortunately, the definition does not form part of the order and is not handled similarly by other Judges. Hence it remains one of the opinions of the nine judges.

However, the majority of the judges have used the term "Information Privacy" and stated that

In the Indian context, a fundamental right to privacy would cover at least the following three aspects:

- **Privacy** that involves the person, such as the right to move freely;
- **Informational privacy** which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual shall have control over the dissemination of material that is personal to him. and
- The **privacy of choice**, which protects an individual's autonomy over fundamental personal choices

We can therefore imply that "Privacy" in cyber space would revolve around "Information privacy" which on how we empower the data subject to make a choice about how his personal data has to be disclosed and used. This is the basis of most Privacy laws including GDPR where "Consent" becomes the backbone of defining the Privacy Protection obligations of a data subject who discloses his personal data to the data controller/processor.

This is also the concept which ITA 2000/8 has adopted when it made reasonable security practice under Section 43A subject to a "Contractual agreement".

PDPA 2018 (Proposed Personal Data Protection Act) tries to break this trend with its approach to the definition of the roles of the data subject and the data controller as we shall discuss in greater detail in a subsequent part of this chapter.

Privacy is a State of Mind

Though the Puttaswamy judgment is a big step towards interpreting anything on "Privacy" in India, we as students of the emerging Privacy laws should momentarily steer clear of the confinement of the

Puttaswamy judgment and look at Privacy with an independent thought process as a part of our quest for Cyber Jurisprudence in the domain of Privacy.

It is accepted that “Privacy” is essentially the right of a person to be “left Alone”. But what is the meaning of being “Left Alone”?. Does it mean that a person needs to be isolated from others from physical proximity to be guaranteed “Privacy”?

It is more appropriate to think that it is not the “Physical Distancing” that makes a person feel “he has been left alone”. It is only when he has a mental feeling that there is no body in his mental vicinity that he feels comfortable of his privacy. It is for this reason that a person who is sitting alone but is being observed through a CCTV camera has no privacy. At the same time, a person who is in the market surrounded by many in close quarters does not have any feeling of Privacy invasion as long as he is anonymous in the crowd.

It is therefore clear that “Privacy” is essentially a “State of Mind” that makes a person feel that there are no prying eyes around him.

Unfortunately human beings are fickle minded in the sense that their preference to be with some body or being alone is not a permanent preference. It keeps changing from time to time and from one person to another.

Some extroverts will not like the silence that comes with Privacy. Introverts donot always remain in a state of meditation and would at least from time to time like to walk out of their isolation and interact with the world.

In such a situation, a question arises how a law can be imposed by a State to write down as a law what is Privacy of its citizens and go about guaranteeing it to the extent that some body who infringes it may face some kind of penalties.

It would be most appropriate if a person defines his Privacy expectations by himself as a part of the societal norm to which he would like to come into and donot expect the Government to make a law for all situations.

For example, if a person A makes a telephone call to B, would it be appropriate for him to consider that the conversation to be private and B cannot share it as he wants. By initiating a call, A should be deemed

to have walked into a conversation out of his choice and hence no privacy exists unless he declares so before the conversation begins.

Similarly when a person puts up a profile picture on Face Book and makes it public, it would be unrealistic to expect that the photo can be considered as “Private” unless his publishing includes some restrictions on copying of the photo etc.

When a person enters the Cyber Space either by visiting a website or entering a discussion room, or fills up a form for availing a service, downloads an app on the mobile, he therefore makes a choice to voluntarily work in a space where the norm is to share information.

Thus what a Privacy Protection legislation can prescribe is only a broad contour of protection and the individual has to manage his own choices by being vigilant. If he is not capable of being vigilant, then he would require assistance of a leader of the society which he would like to enter.

This concept has been captured in the PDPA 2018 by defining the relationship between the Data Subject and the Data Controller (as used in the international data protection legislations) as one of a Data Principal and Data Fiduciary.

In summary we can therefore understand that “Data Protection” can be approached either as “Protection of Data” or as “Protection of Privacy Right through protection of relevant information” and accordingly the laws have to address the requirements.

Since “Data Protection” in either form is dependent on “Technology”, the changing scenario of technology has an impact on the Data protection laws. To appreciate the Data protection laws as we have today around us and what is emerging in India in the form of PDPA 2018, we need to also look at some of the key developments in information technology that is occurring around us in the form of Quantum Computing, Artificial Intelligence, Big Data, IoT etc. The next part of this chapter therefore focusses on providing a basic understanding of these emerging technology developments in the context of how it may affect the domain of “Data Protection”.

Part B: Technology Trends

We have already discussed that “Data Protection” Laws apart from protecting “Data” which is in electronic form, try to afford protection to Privacy of citizens in the physical space from any adverse

effects arising from the Cyber Space. In this context, Data Protection Laws try to provide protection to the "Privacy Rights" of a Physical Society citizen by managing "Information Privacy".

ITA 2000/8[iv] has a legal definitions for "Data", "Information" and "Computer" under different subsections of Section 2. The essence of the legal definitions is that "Computer" is a device that functions by manipulations of "impulses" and includes all input, output devices, processing and storage devices, software and communication facilities.

Interpreting the definitions of Data, Information, Computer, Electronic Document, etc in ITA 2000/8, without conflict to the meaning derived therefrom, "Data" can be understood as

> *"A sequence of binary expressions which are capable of being interpreted into a human experience through the use of compatible software and hardware."*

[P.S: This is the interpretative definition of "Data" according to Naavi, the author]

With the development of technology, "Electronics" is being embedded into the functions of almost any of the devices which we use today, be it the Car or the Washing Machine or the Microwave oven. Hence "Data" is captured, stored, processed and transmitted by many of the electronic devices that we use today in normal activities. Some of these devices may use special technologies which require us to understand the interpretation of Data Protection laws in these different technological environments.

Let us therefore try to explore some of these technologies briefly so as to open our minds to the complexities or challenges they present in data protection regulation.

I. Quantum Computing

Quantum Computing as a technology refers to the ability to process data which is stored in "Quantum Bits" (Qubits).

A "Bit" is a unit of some thing that can take one of the two binary positions of "Zero" or "One". In the ordinary hard disk, a "Bit" is represented by a unit of a surface which can take an independent magnetic position either in one direction or the opposite direction. When such bits are placed in a series, they become "Data".

“Data” can be expressed in many forms, the magnetization of the surface being one such form. CDs use a different technique like creation of “Pits” and “Lands” so that light reflections from these can be interpreted as binary expressions.
Law does not distinguish whether the device uses “pits” and “lands” or “magnetic orientation-North” and “magnetic orientation –south” to represent the “Zero” or “One”. Hence “Data” is platform independent.
The Computers have not only the “Data Storage” functionality but also the “Data Processing” functionality. In “Data Processing”, electric current is passed through a circuit board and its path may alter the status of an electronic document. When an electronic document changes from “Version 1” to “Version 2”, we say that the document has been “Processed”. This change means that the binary sequence of Version 1 is re-set into an alternate binary sequence of Version 2. Both Version 1 and Version 2 are static positions of a sequence of binary states of a set of bits. The modification is through the “Processors”.

The “Processor” uses a special arrangement of what students of Physics call as “Transistors”. A transistor is a tiny electronic device that can allow current to pass or block current to pass depending on the status of one of the elements in the transistor. This is what can be called a “Binary State” of a transistor.

We can therefore consider that “Transistor” is the heart of a computer and is responsible for the processing activity.

When “Transistor” was first invented, (1947) they were in the form of “Cathode Ray Tubes”. Gradually they were converted into “solid state devices” (1960). These solid state devices were then built into “Integrated Circuits” (ICs). These ICs later became “Printed Circuit boards” (PCB) where the entire circuitry was created like a line drawing where current could flow, be stopped, or be diverted into different segments of the circuits. The PCB became units that could be assembled together so that multiple binary functions could be conducted. As time went on these PCBs became smaller and smaller and the effort was to put millions of transistors in a small “Chip”.

At first glance, it may be difficult to recognize that inside every computer are millions of transistors. Data is also a sequence of transistors in zero or one state. Eight such transistor sequence is a byte.

This quest for miniaturization has now gone through the nano technology phase and entered the “Quantum Computing Phase”. In “Quantum Computing”, the “Bit” that holds the binary position of zero or one is not a magnetizable space. It is as small as an “Atom” or a “Nucleus” or an “Electron” in an atom.

In “Nuclear Physics”, we know that an atom consists of a nucleus and electrons going around it in different orbits. These particles need to always keep spinning over its own axis in order to remain stable even if they also rotate around another axis just as the Moon rotates around its own axis and also rotates around the earth and earth rotates around its own axis and also rotates around the Sun.

In the case of planets their spin direction is always in one direction and does not change. But in the case of electrons and nuclei, it is possible for the spin direction to change from clockwise to anti clockwise.

Quantum computing uses this principle where the “Direction of Spin” of an isolated electron or a nucleus is recognized as a binary expression of “Zero” or “One”.

Computing based on such particles being the representative of the “Data Bit” is “Quantum computing”. These “Bits” are called Qubits. Qubits could be Atoms or electrons or nucleus. They can be even other sub atomic particles like the neutrons and protons or molecules which contain a combination of sub atomic particles.

Let’s leave the discussion of “Quantum States” of the particles to the experts in Physics who are the fore fathers of “Computer Engineers” of today and look at the legal implications of Quantum Computing.

From the legal perspective, as long as we have a device which can read the quantum state of a Qubit as zero or one, it can continue to process or store data in binary form as we are accustomed to now. The Law does not need any change to be made on this account.

However, these sub atomic particles are extremely unstable and keep changing their spin status randomly. Their stability increases when they are cooled down but not to the temperatures that we are accustomed to living but to the levels of a near -273 degree Celsius which is called “Absolute Zero”. “Absolute Zero” is a theoretical impossibility and the temperatures used for Quantum Computing is a few nano degrees above absolute zero.

It is therefore possible for creating a “Cool Chamber” in which “Qubits” are held and function for computing purpose in Quantum Computing.

The benefit of Quantum Computing is not limited to “Miniaturization”. But Quantum Computing leads to a dramatic increase in the processing speed. If we replace binary bits with Qubits, the processing can

work at around 100 million times faster. Researchers in Google have created a 72 Qubit experimental system while IBM is experimenting with a 50 Qubit system. Compared to "Classic Computing" these computers are equivalent to super computers having millions of fastest chips that can function as a super computer.

A 64 bit quantum computer has a computational power of 2^64 (2 multiplied by itself 64 times) times faster than our 64 bit classical computer.

II. Super Positioning

The reason why Qubits can function faster than classic bits is that a Qubit can be assigned both the position of Zero and One simultaneously with a probabilistic value within acceptable error range, unlike the classic bit that can assume at any point of time either zero or one. This property is called "Super Positioning" of Qubits.

Certain processing algorithms can use this "Super Positioning" property and can speed up the processing. From the legal perspective, this "Super Positioning" introduces an element of "Uncertainty" about data.On a witness platform if the witness is asked a question

Is this Qubit in "zero" position or "One" position?, and he answers it can be both Zero or One, then the classical advocate will shout, "You can only say Yes or No. You cannot answer Yes and No". A classical Judge may therefore find it difficult to appreciate the evidence.

Though this appears to be a serious problem, Naavi has explained [v] that Indian system of Section 65B of Indian Evidence Act surmounts this problem and can be effectively used even if evidence is being processed or stored in quantum computing platform.

Some of the problems get resolved because "Quantum Computing" is used in conjunction with Classical computing as a back room processing assistant and hence presentation of any data as evidence may ultimately happen in the classical computers in the ordinary user's domain.

III. Entanglement

Another property of Quantum computing that has attracted attention is the property of "Entanglement". This is another concept more suitable for scientific fiction story writing but we the Cyber Law Specialists need to learn these technology aspects to ensure that the Cyber Laws as we know keep pace with the development.

In simple terms, “Entanglement” is a property of a sub atomic particle where every such particle has a counter existence. In other words, two sub atomic particles separated by a distance seem to be so “Entangled” that change of status of one of the particles induces an automatic change of status of the other particle in the reverse direction.

If “Particle A” is spinning in a clockwise direction, then its entangled partner namely “Particle B” is spinning in counter clockwise direction. If now we change the spinning of Particle A to anti clock wise, then Particle B automatically changes its spinning status to clockwise. This may look strange but has been proved true by Quantum Physicists.

The property of QuBits to exhibit the “Entanglement” behaviour could be another area of uncertainty that a Classical advocate and Classical Judge need to contend with.

Again the use of Section 65B of Indian Evidence Act circumvents the problem if we understand the technology of Quantum Computing and allows the interpretation of Section 65B as presented by Naavi in his book “Section 65B of Indian Evidence Act Clarified”[vi] is universally accepted.

In the Data Protection regulation therefore, when Quantum Computing is used for any part of Data Processing, security in terms of Availability, Integrity and Confidentiality as well as authentication and non-repudiation needs to be addressed differently.

The new concepts could seriously clash with the principle of Criminal Justice such as “Proof Beyond Reasonable Doubt”. Since under quantum computing, we will be dealing with “Probability” and not “Certainty”, it automatically accepts that there is no “Proof Beyond Reasonable Doubt”. At best we can re-define “Reasonable” as 60% or 80% probability of reasonableness.

IV. Artificial Intelligence

While Quantum Computing may be a little time to come into our normal usage, Artificial Intelligence has already made big inroads to the activities of companies.

Artificial intelligence (AI) in the real sense means an ability to replicate human intelligence in machine operations. It requires the computers to respond to dynamic situations through a cognitive ability to analyse the situation and apply the best possible solution including those which have never been tried before.

AI should therefore include speech recognition, learning, planning and problem solving.

While it is possible to load a computer with “Knowledge” in the form of how to respond automatically to known stimuli, where there is a need to apply reasoning and accept the most optimal of the available solutions it is a challenge.

Human Beings often work on “Instincts”. Most of the “Instincts” are built on sub conscious memory and donot necessary come out of extra sensory perceptions.

In the case of computers, “Machine Learning” is a process that builds memory out of past incidents and is like a human being who acquires experience as we pass through life. This may be automatic in the sense that the machine may document its experience by itself without a further human input and use that for future decision making.

However the inputs if any as a post facto approval as well as how the Computer should interpret the automated machine observations is programmed through a computer logic created by a human being. Every act of an AI led machine therefore has its causation through programming done by a human being.

The machine perceptions depend on the sensory inputs to deduce different aspects of the world. Humans not only see and hear things but also “feel” things. This sense of “feeling” will not be possible for a computer. “Feeling” may not always lead to the correct decision making and delinking it from the decision making process may actually lead to better decisions in certain circumstances. But it is a philosophical question if “Feeling” must be part of every decision making and an efficient decision from the perspective of the society cannot be divested of the “feeling”.

The AI can therefore be very near human intelligence and good for routine jobs but may still fall short of human intelligence at the highest level. The AI works on “algorithms” that are capable of quickly analysing different data inputs and processing them into a decision output. The humanoid robots like the “Sophia” have presented themselves well in the society. However, many of the accidents that have been reported from the Robotic operations in the industry and unsubstantiated reports from Japan about a rogue military robot [vii] have raised the concerns of AI malfunctioning.

Presently research is still going on in the field of “Artificial Neuron Network” which is an attempt to replicate the biological neuron network. The “Speed” factor has been addressed by the development of the

"Quantum Computing technology" and today's AI led platforms are capable of mimicking the human intelligence to a large extent.

Adaptive resonance theory (ART) is a particular philosophy driving unsupervised artificial neural network models. It uses a specific architecture, often useful in some types of neural networks, to try to build the capacity for new learning while keeping in place fundamental existing models.

Experts describe adaptive resonance theory as partially an effort to remain open to new learning without sacrificing knowledge of existing patterns – hence the words "adaptation" and "resonance."

While we can leave the technology experts to continue their research in replicating human intelligence and to the scientific fiction writers to flag the risks, Cyber Law and Data Protection Law makers need to factor in the need to "Fix Responsibility" for AI led decisions in data processing.

In ITA 2000/8 it is clearly laid down that an action of an automated system is attributed to the person who caused the system to act in the specified manner. In Other words, the liability arising out of the activities AI led machines will be that of its "Owner" and the "Software Developer" based on the software transfer contract.

Law has to still decide how "Data Being seen by an AI machine" be treated under Data Protection laws. Will it be a "Data Disclosure"? should there be some form of contractual commitment by the AI machine before it is allowed to read the data? Etc., need to be sorted out.

For the time being, we can resolve the legal issue by substituting the AI machine with the person to whom its action is attributed, to fix the liabilities arising out of AI operations. We may have to wait several more years to develop Jurisprudence in this matter.

Some experts argue that in future we do not need Courts, Lawyers and Judges since "AI" can take decisions based on the written law, submitted arguments and evidences. But if such a day comes then the human element in judgements which today enable Judiciary to be dynamic will be killed.

While adopting Cyber Law to the emerging technologies we need to also incorporate the discussions on "Philosophy and Purpose of Law" and consider if the change is desirable or not.

V. Big Data:

Big Data is a term used when huge quantity of data is collected from different sources and the accumulated data is available for analysis to reveal patterns, trends and associations that are not visible when data is seen in silos.

The Source of Big Data is the information transmission nodes and the public data storage points. It could involve mostly “Anonymous Data” or “Pseudonymous Data” and if so, it is outside the purview of Data protection laws.

Beyond these, data is stored in private custody, behind Firewalls and unless it is transferred from the place of creation across an open network, it may never become accessible to Big Data Sniffers. This private data is normally protected and hence should not without permissions from the data owners, be part of the big data.

When Big Data Sniffers “Mine” for data, they may not target any specific type of data or an individual. The data collected from an omnibus data collection drive may later get filtered and classified into different types of data and tagged accordingly for further harnessing.

If however, an acquirer of “Big Data” from the public space also has access to some private data and thereby renders the data “Identified”, then there is an element of Data Protection regulation that may get invoked.

Components of Big Data are

a) Personal Data collected from Individuals including individualized data such as emanating from devices embedded to the human body such as Wearable s and Medical implants.

b) Corporate Data which includes business information as well as personal data of individuals in the hands of a corporate either as custodians of employee data or as intermediaries processing data of customers and public.

c) Environmental data including those collected from Weather satellites, Mapping devices, CCTVs in public places etc where the primary aim is not to collect personal data but it becomes part of the overall data collected.

d) Meta Data which is “Data about Data” which involves transactions of Netizens, tracking of data movement over a public network and includes “Log Records” of all kinds. Though this data is impersonal at the time of collection, they are amenable to further analysis and conversion from a de-identified state to an identified state.

Big Data is a concern for Privacy Protection since the consent that a data subject might have provided when he shares his data with a service provider may become redundant since Big Data Analytics may identify a data simply from its own intelligent computations of the Big Data. With the identity the data subject may also be “Profiled”. The “Profile” may later be used for decision making that may affect the data subject.

Whether such analytics is accurate and inferences drawn are correct depends on the strength of the AI algorithms that run behind the scene. But Privacy Activists still consider that “Any kind of profiling of an individual whether accurately or otherwise” is an infringement of Privacy.

This was part of the controversy in the Cambridge Analytica incident [viii]where data collected for one purpose was used in another context in the form of profiled data.

Data Protection professionals working with Big Data need to therefore ensure that while they work with data and its aggregation, personal data is never identified with a living individual. Otherwise they may be infringing on the data protection laws. In fact most data protection laws consider re-identification of pseudonymized/de-identified data as an offence.

The conflict between Data Scientists and Privacy Protectionists will be like the conflict between “Freedom of Speech” and “Right to Privacy”. It is unlikely to be resolved to the satisfaction of the industry.

The Concept of “Legitimate Interest Policy” which Personal Data Standard of India (PDPSI) [ix]considers as a key policy control tries to address this conflict to some extent.

VI. Internet of Things (IoT)

Internet of things (IoT) is the term which is being used to describe the world of consumer goods that are connected to Internet. The devices that can be classified as IoT include CCTVs, security systems, cars,

smart electricity meters, the cars, the microwave ovens, lights, speaker systems etc. The devices may also include “Baby Monitoring Cameras”, Medical devices which generate what is considered “Sensitive Personal Information” requiring special efforts of protection.

It is estimated that there will be are more than 300 billion devices that can connect to internet by 2020. The Ipv6 system enables the connectivity of these devices with a unique IP address and hopefully support this new world of connected devices.

Primarily the connectivity is designed to enable the owner of the device to operate it remotely through the internet and probably with an app on the mobile. Hence the data associated with the activity of an IoT device will be traceable to the activity of an individual and hence becomes part of his activity profiling.

Hence IoT data becomes part of the data that needs to be protected for “Privacy Protection” .
Additionally, in certain cases, the connectivity may be linked to the manufacturer for the purpose of maintenance and updation.

Because of this connectivity IoT also gives raise to exploitation by Cyber Criminals for committing Cyber Crimes including using the network to launch Denial of Service Attacks. Hence there is a need to develop an effective security system to ensure that the IoT connected network.
In terms of Data Protection Compliance of an organization therefore, if the organization is either a manufacturer supplier of IoT devices or a supplier of intermediary services, it is necessary to ensure that the data inflow from these devise need to be factored into the data protection regime.

The device identity itself may not be considered “Individually Identifiable Personal Information” and therefore data flowing in with only the device identity can be considered as outside the purview of Personal Data Protection. However, if in the organization, the device ID can be mapped to the purchaser who is an individual, then the data assumes the nature of Personal Information.

Hence such organizations need to keep the “Purchaser-Device ID Mapping” which is part of the “Maintenance Data base” secure from the general data that may be flowing in about the performance of the device, which is part of the “Big Data” that the organization may keep accumulating.

The current Data protection laws expect “Privacy By Design” which can be extended to the designing of the IoT devices and their communication systems. It may be necessary to ensure encryption of data flowing from the device to the central command center or to the consumer owner so that security in

transmission is ensured. If some data has to be stored within the device, any exfiltration of this data especially through remote log in must be secured. Failure in this respect could be considered as failure of the Data Protection at the manufacturing end.

If IoT devices are manufactured in one country and sold across the border, then the company has to be also mindful of the cross border data transfer restrictions in the country where the products are used.

Thus IoT s provide a challenge for Data Protection because of the numbers involved, their wide geographical spread as well as the general ignorance of the consumers in following data security practices.

The laws may also overlap between Consumer Protection, Cyber Laws and Data protection laws and law makers need to carefully design the laws to cover all lose ends without hurting the fundamental objective of the device which is to provide a "Consumer Service".

VII. Block-Chain Technology

"BlockChain" is a term which became popular as the platform that supports "Bitcoin" as a "Crypto Currency". Technologists today are trying to present "Block Chain" as a technology and "Bitcoin" as only a product based on the technology. Hence there is an attempt to find other use cases in which the "Block Chain System" can be used. It is in this context that we can take a quick glance at this technology.

Block Chain essentially is a system where several users come together in a network to maintain a decentralized ledger of events with an agreed procedure for adding new transaction to the current ledger as an authenticated event. The transaction as and when it occurs is broadcast to all the members and when a majority of them duly add it to the current ledger as per the agreed procedure it is deemed to have been authenticated.

In a "Bitcoin" transaction, if A transfers 1 bitcoin to B, this transaction is broadcast to all the Bitcoin nodes. Each of the nodes try to create a list of transactions since the last successful "Block creation". They then proceed to add a variable (nonce value) and calculate a hash value of the block. If the hash value satisfies the criteria fixed by the block creation, the person is considered to have succeeded in creating a new block which gets added to the earlier chain of blocks and he is rewarded with an issue of new bitcoins as per the rule. (This is the mining activity). If the hash value does not meet the criteria, the nonce value is changed and a new hash value is calculated and so on.

All successful creation of blocks is added to the previous block chain and will contain the identity of the successful miner. The Bitcoin protocol ensures that the transactions and the block are digitally signed for authentication and encryption. The identity of the parties is in the form of encrypted private key of persons and hence does not contain the identifiable personal information.

This concept of a “Group of people” expressing endorsement of an event by adding their approval one after another can be called the “Block Chain technology”. However for a “Block” to be called “Successful” and added permanently to the transaction data base, it is necessary for a minimum number of people to authenticate the transaction.

In the Bitcoin block chain the nodes who participate in the authentication are manned by “Public” and they donot hold any specific authority to approve. On the other hand in a “Private Block Chain”, the power to approve may be restricted with a few designated persons.

One of the essential features of the “Block Chain Technology” is that an approved transaction gets added to the earlier set of transaction and the transaction chain grows. It is like a ledger which is brought for signature to a person and he signs it and passes on the entire ledger to another person.

In a normal Banking transaction, we create “Transaction Vouchers” which move from one authenticator to another and when fully approved, some body maintains a centralized ledger where it is added. Only the “Voucher” is transmitted and not the “Ledger”.

In comparison, if Block Chain technology is to be used, the authenticated ledger itself has to move with every successful authentication.

Such a system may not be ideal in all kinds of transactions but may be of use in recording transactions which have a short life cycle.

From the Data Security point of view, if every authentication is digitally signed with hashing of content with private key and encrypted with the receiver’s public key, then the content is protected against loss of confidentiality in transit and also incorporate the authentication of the sender.

If however the content is not encrypted, depending on the nature of the content, there will be “Privacy” issues.

Some of the Banks in India are reportedly experimenting on the use of Block chain technology for some part of their transaction recording. But these experiments may not be similar to the "Decentralized" public ledgers maintained in the case of Bitcoin where several persons are authorized to interact with the block and authenticate. What is normally done is to use the system of "Add authentication and move the entire file to the next person" in a sequential manner.

Every transmission is digitally signed, and encrypted with the public key of the addressee. The recipient decrypts the content with his private key, adds his comments/authentication, digitally signs the previous message with his added content, encrypts with the public key of the next addressee and forwards it until it reaches its destination at the end of the life cycle when it is archived.

In India, if the digital signature is one which is approved under ITA 2000/8, legal sanctity can be built into the system.

In summary we can take note that there are interesting technological developments that are occurring around us which leave a significant impact on the Data Protection aspects and those who frame the laws and those who need to follow them need to ensure that laws are not distorted due to mis-interpretation as well as emergence of new technology that changes the foundation of the law as enacted.

Part C: Some Key Data Protection Legislations

In this section we shall briefly discuss three important data protection legislations that are relevant in India namely HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Act) and PDPA 2018 (Personal Data Protection Act 2018).

Off these, PDPA 2018 is the proposed draft law for India. HIPAA is the law applicable for the processing of Health Information of US citizens and is relevant in India since India is a hub for processing of such data through Business Associate Contracts. GDPR is the legislation of the European Union and relevant to Indian Companies if they handle data of EU citizens.

I. HIPAA

USA follows a system of sectoral Privacy Protection laws. HIPAA is the Privacy Protection Act applicable to the Health Care sector. It has been in place since 1996 and was further fortified by the HITECH Act (Health Information Technology for Economical and Clinical Health Act) in 2009.

HIPAA had three distinctive objectives. First was “Administrative Simplification” in the digital health record scenario by mandating standards for identifying participants in health care industry, recording electronic transaction, identifying diseases, medical procedures, drugs etc., in the creation of Electronic Health Records (EHR). The second was the “Privacy Rule” for handling individually identifiable health information and the third was the information security rule for protected health information (PHI). Additionally some reforms were also brought through this legislation in the Health Insurance sector to ensure portability of insurance schemes when people move from one scheme of insurance to another due to job changes etc.

HIPAA was applicable to certain entities referred to as “Covered Entities”.

The “Covered Entities” are the following

1. Health Care Providers
2. Health Care Clearing Houses
3. Health Plans/Insurance Providers

Before HITECH Act came in, “Business Associates” who process PHI on behalf of the covered entities were not directly under the regulations. The Covered Entities were responsible for the compliance at Business Associates. Fines and penalties were imposed by the regulator namely the HHS (Health and Human Services department) on the covered entities. The Covered entities imposed the responsibilities along with indemnity provisions on the Business Entities through the mandatory “Business Associate Contract”.

Under HITECH Act, the Business Associates have been brought directly under the regulations and are liable for penalties in case of non compliance.

However, when we apply HIPAA-HITECH Act in the context of Indian Business Associates, the incidence of the compliance provisions is still through the Business Associate Contract (BA Contract) since HHS does not have legal jurisdiction on the Indian Companies.

Covered Entities

HIPAA defines the three types of covered entities to which the Act is applicable.

Health Care Provider is any entity that provides health related services. It includes any person/entity who/which while providing health care services, generate, store and transmit health information and includes hospitals, physician practices, dental practices, health plans, laboratories, health care clearinghouses, pharmacies, etc

Health Care clearing house includes a public or private entity that processes or facilitates the processing of non standard data elements of health information into standard data elements routes electronic data between providers and payers.

Health plans include any individual or group plan that provides or pays the cost of medical care. Includes only group health plans which has 50 or more participants and is administered by an entity other than the employer.

Organizations which have any of the above activities along with some other activity are called “Hybrid Entities” and such entities if they are able to segregate the health Care Component from other activities, will be considered as a Covered entity for that part of the business alone.

Business Associate is any organization which under a contract with a covered entity processes the individually identified health information which is the subject matter of protection under the Act and is called Protected Health Information or PHI.

Essence of HIPAA-HITECH provisions include Administrative Simplification, Privacy Rule and the Security rule which are briefly explained below.

Administrative Simplification

The principle purpose of administrative simplification for Health Insurance is to facilitate electronic data interchange through standardized documentation and reduce costs of administration. In order to facilitate this, covered transactions such as Health Claims, Enrolment and Disenrollment, First Report of Injury etc have been standardized. Unique identification codes have been allocated to patients, medical practitioners including hospitals. Standard codes for Drugs, Medical Procedures etc which were otherwise available in the industry are used.

With such standaridization, easy interchange of data from the hospitals to pharmacies and the insurance industry was sought to be achived, to bring better economy in the operations as well as control on frauds.

Privacy Rule

The Privacy Rule under HIPAA is that “Protected Health Information shall not be used or disclosed by a covered entity except as otherwise permitted under the provisions, required under the provisions or authorized by the data subject.

A data subject has the right to authorize disclosure of his data while he is in a mental condition to provide such authorizations. Such authorization can also be provided by a guardian on behalf of a minor.

The regulations require disclosure of information to the HHS as the regulator and to the data subject himself under certain circumstances. Such disclosures are “Required” and not providing them would be a contravention of the law.

Other than the above circumstances, HIPAA prescribes that PHI may be disclosed in the following circumstances.

1. To the Individual for Treatment, Payment, and Health Care Operations;
2. When there was an Opportunity to Agree or Object which was not exercised by the individual
3. Incidental to an otherwise permitted use and disclosure;
4. Public Interest and Benefit Activities; and
5. (Limited Data Set for the purposes of research, public health or health care operations.
6. Requirement of law

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Disclosure from one covered entity to another is also permitted because both are bound by the law.

When disclosure is made to Business Associates or Sub Contractors, they should be bound by a BA Contract in which the same level of safeguards as are required to be followed by the covered entity are imposed on the BA/ sub contractor.

This privacy rule is applicable for the processing of PHI (individually identifiable health information) of US citizens.

PHI in encrypted form is considered as “Secured PHI” and is not subject to the regulatory controls that are required for PHI.

A personal health information is considered “Identifiable” if certain parameters of identity such as the name, address etc are associated with it.

It may be noted that the origin of PHI is in data which contains some health information to which an identity parameter is associated with. In most other privacy regulations, the origin is with the name of an individual to which other parameters of identity are associated with. This distinction makes HIPAA’s definition of PHI more clear than the definition of protectable information under other regulations.

HIPAA clarifies that “Health Data with any of the identity parameters indicated under the regulations is PHI”. In other regulations, “Name with any of the identity parameters is considered as “Protectable Information”.

HIPAA lists 18 parameters that are considered as identity parameters. However other regulations donot always specify an exhaustive list of identity parameters. In the days of AI, given the efforts most of the information can be traced to an individual and hence most of the information associated with a human being also becomes “Identifiable”. This expands the scope of applicability of the regulation wider than in the case of HIPAA.

Any information which is devoid of identifiable parameters are considered as “De-Identified” information.

However, in laws such as GDPR/PDPA 2018, the scope gets limited by the nationality of the individual and the geographical area from which the activity of an individual gets recorded. HIPAA’s limitation is on the basis of the entity being a “Covered Entity” and the “Information being related to health of an individual”.

Security Rule

In order to ensure that the “Privacy Rule” is followed, HIPAA prescribes a well defined “Security Rule”. This “Security Rule” is made of 22 Standards. 15 of these standards contain a more detailed “Implementation Specification”. 7 Standards donot have specified implementation specifications. There are 45 such implementation specifications. 23 of these are tagged as “Required” and 22 are tagged

"Addressable". These 45 specifications with the 7 standards without specifications form a set of 52 information security controls prescribed under HIPAA.

"Standards" and "Required" Implementation specifications are mandatory. "Addressable" implementation specifications are to be complied with but the organization can either

a) Find alternate ways of compliance other than what is indicated in the implementation specification
b) Document why the subject implementation specification is either not relevant to the organisation or Document how the specification has already been complied with by any of the other implementations.

If however the organization finds that the addressable implementation specification is reasonable and appropriate for the organization, it must be implemented.

A detailed discussion on the security rule is out of scope of this discussion.

Compliance officials

HIPAA requires that the organization assigns the responsibility for compliance to designated persons and hence it is mandatory to appoint a "HIPAA Compliance Official" to oversee the compliance. Ideally there can be a "Privacy Compliance Official" separate from a "Information Security Compliance Official". Manpower training is also a mandatory aspect of HIPAA.

Data Breach Notification

It is one of the important aspects of HIPAA that any data breach has to be notified to the data subject as well as the HHS. The organization has to disclose the breach on its website. Where the number of data breaches are high, there would be a need for the organization to place a disclosure notice in the media also. The HHS reports data breaches to the Government at the end of the year.

Failure to notify is also a matter of non compliance of the regulations.

Loss of De-identified information and Encrypted Information does not require Data Breach Notification.

Penalties

Under HIPAA, both Civil and Criminal penalties are possible. Civil Penalties may extend from US $100 to 50000/- per violation depending on the type of violation subject to a maximum os $ 1.5 million per year per type of violation.

For repeated violations and multiple violations of the rule, the penalties could be higher.

Criminal Penalties could extend to 10 years of imprisonment and fine of upto $250,000/-
Under HIPAA no private Civil Action is recognized.
In summary it can be stated that HIPAA is a sectoral Privacy protection law applicable to US covered entities and extends by contractual obligations to Business Associates and Sub Contractors. Penalties are heavy and may arise for noncompliance even where there is no data breach.

Over a period HIPAA has become a "Best Practice Standard" for health care industry across the world.

In India, there are a set of EHR guidelines which are in operation and are normally expected to be followed by Government establishments. A new law called DISHA (Digital Information Security for Health Care Act) is in draft stage. ITA 2000/8 recognizes Health Data as "Sensitive personal data" under Section 43A and expects "Reasonable Security Practice" to be applied. Such "Reasonable" security practice may be equated to the recognition of HIPAA as the best industry practice. As a result HIPAA is considered relevant for Indian Heath Care industry. As and when DISHA[x] becomes a law, it may incorporate most of the provisions of HIPAA.

III. GDPR

GDPR has created waves of excitement across the world as the most fierce Privacy Regulation ever enacted in the world. GDPR stands for "General Data Protection Regulation" which replaced the EU Data Protection Directive based on which several EU Countries had enacted "Data Protection Acts" for their respective countries. It became effective from 25th May 2018 and since then caused a huge turmoil in the global IT industry.

The reason for the commotion is that GDPR imposes civil penalties which at the highest level can go upot 4% of Global turnover of a company and such penalty can be imposed merely for the non compliance aspects of law even when data breach is not recorded. Further by giving an indication that the law is applicable to companies outside EU, it shook up the IT companies even in India.

It is to be noted that EU Privacy Protection Directive was already in existence and had incorporated most of the Privacy Principles which are also indicated in the GDPR. Companies were already in compliance with the directive and had established several legal instruments such as US Privacy Shield, the Standard Contractual Clauses, Binding Corporate Rules etc to remain compliant. Now similar provisions are required to be modified and extended to meet the new requirements under GDPR.

However the huge penalty that GDPR can impose created a panic amongst the global companies since they were unprepared for full compliance despite a complete 2 year notice that GDPR would be effective from 25th May 2018.

GDPR [xi]consists of a total of 99 Articles spread over XI chapters and has been discussed in great detail by the undersigned which may be referred at the Privacy Knowledge Center. (www.privacy.ind.in). We shall briefly discuss the essential features of GDPR here.

The applicability of GDPR is however defined as under:

1. GDPR does not apply for processing of personal data which is in the course of an activity which falls outside the scope of the EU law.
2. GDPR does not apply to purely personal and household activity
3. GDPR does not apply to competent authorities for the purposes of the prevention, investigation,detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
4. GDPR applies to the processing of personal data in the context of the activities of an establishment in the EU regardless of whether the processing takes place in the Union or not.
5. GDPR also applies to the processing of personal data of data subjects who are in the Union by an entity not established in the Union, where the processing activities are related to:

    (a) 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

    (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

GDPR in essence

a) Established a Recognition of Data Protection Rights of the Data Subjects
b) Reiterated the Principles of Privacy Protection to be followed by Data Controllers and Data Processors
c) Highlighted the responsibilities of a Data Controller and Data Processor including the Mandated the Compliance requirements, Cross border data transfer restrictions etc
d) Indicated the remedies available to the Data Subjects and the penalties that may be imposed on the Data Controllers/Processors
e) Established a Compliance Structure with Supervisory authorities, Codes of Practice etc
f) Provided for necessary exemptions for reasons of National Security, Public Interest etc.

Data Subject's Rights:

Data Subject is the person who provides his personal data which is collected and processed by other entities. The Data Subject is entitled to a transparent manner of collection and processing. "Consent" which explains what information is collected and how it is processed etc is an essential right of the Data Subject.

Data Subject is entitled to **"Access"** the data about himself which is being processed and also demand **accuracy** and **rectification** as may be required.

Data Subject is also entitled to **"Port"** his personal data out of one processor/controller to another and also insist on **"Right to Forget"** which could mean a right to demand erasure of his personal data held by a Controller/Processor. He can also impose restrictions on the processing of his personal data.

In all these aspects, though the Data Subject appears to "Own" his personal data, unlike some other laws (Eg: California Consumer Privacy Act, India's DISHA draft Act), Personal Data is not declared as a "Property". The Right to use the Data is transferred to the Controller through a "Contract of Consent".

GDPR therefore considers that "Data Subject's right" on his personal data is a "Right" that can be selectively transferred to another person and such transfer is revocable and transferable to another person.

In data processing, the end product of processing is often a "Profile" of the data subject which is a value added product developed by the processor. This "Profile" is a derivative of the raw personal data provided

by the data subject and hence may be claimed back by the Data Subject under the “Portability” or “Erasure” rights. Since this may have a conflict with the IPR of the Data processor, there is need for the industry to discuss and sort out this conflict with the IPR laws.

Principles of Privacy Protection:

The Principles of Personal Data Protection under GDPR is the well established list of six principles namely

a) Processing shall be Lawful, Fair and Transparent (Transparency, Fairness and Lawfulness)
b) Collected for specified and legitimate purposes and limited to the indicated purpose only (Purpose Limitation)
c) Collection shall be limited to want is adequate and relevant to the purpose (Data Minimisation)
d) Adequately secured against wrongful modification and use (Accuracy and Security)
e) Kept only as long as it is necessary for the purpose and not any longer (Storage limitation)
f) Controller being able to demonstrate compliance. (Accountability)

Responsibilities of the Data Controller/Data Processor

GDPR recognized that the entity which has the right to decide how the personal data of a data subject has to be processed and for what purpose is called the “Controller”. The principal responsibility to protect the rights of the data subject also lies with the Controller. When the data is passed on to a “Processor”, the processor is mainly responsible to the Controller through a contract, though the GDPR liabilities do attach to the processor also. Apart from the Controller and the Processor, GDPR recognizes a role for a “Recipient” who is the person to whom the personal data is disclosed.

When the data subject first hands over his personal data against a consent form signed with an entity, that entity is deemed as also a “Controller”. If his role is limited to collection of data only after which it is passed on to another entity which determines the purpose of processing, then both would be “Joint Controllers”. Similarly, if the “Processor” determines how the data is to be processed and the purpose, he would be the “Controller” also. Since “Receipt”, “Storage” and “transmission” is also considered as “Processing”, all “Controllers” are also “Processors” while the reverse may not be true.

Controller or the Processor is expected to ensure that “Privacy” is protected “By design”, meaning that by default all processes should be geared towards privacy protection. Every organization should have a “Data Protection Officer” (DPO) assigned with the responsibility to manage the responsibilities. Such

DPO could be appointed as an external contractual consultant also and one DPO can be appointed for a group of entities. The entity should conduct a “Data Protection Impact Assessment” if necessary from time to time to make an assessment of the risks of noncompliance of GDPR and initiate necessary action to mitigate.

GDPR recognizes that the Controller/Processor has certain “Legitimate Interests” in processing which can be protected with a structuring of a proper Consent contract with the data subject.

Additionally the organization needs to have a comprehensive Privacy Policy to define its Compliance stance which should be notified to all the employees and external stake holders to the extent their cooperation would be required. The entity should also put in place a comprehensive Information Security Policy equivalent to as per the best industry practice. ISO 27001 or HIPAA or BS 10012 could be some standards that the organizations can pursue.

For Companies in India, the Personal Data Protection Standard of India (PDPSI) is a framework that encompasses the best practices of standards like BS 10012, ISO 27001 or HIPAA and also the Indian laws such as ITA 2000/8, the proposed DISHA and PDPA 2018.

More details of PDPSI is provided in subsequent part of this lesson.
Where a data breach is identified, a processor has to keep the Controller informed immediately and the Controller has to inform the Supervisory authority within 72 hours. In most of the cases, the data breach has to be informed individually to the data subjects also.

In order to meet the requirements of GDPR, a company needs to also maintain a proper Incident management system as well as Disaster Recovery and Business Continuity plans. It has to also ensure a robust HR policy incorporating adequate training and sanctions for preventing breach through negligence or insider involvement.

The Data Controller/Processor should also be able to respond to any complaints from data subjects as well as enquiries for queries regarding whether the organization is processing the data subject’s personal data or not. If the data subject likes to port the personal data or erase the data, necessary action needs to be initiated. The Data Protection Officer would be the contact person who will receive such queries from the data subject and also maintain the relationship with the supervisory authorities.

The Controllers and Processors need to document their compliance activities and also ensure that they cooperate with the regulatory agencies when any information is called for.

The Indian regulation of PDPA 2018 as proposed takes into account most of the good practices suggested in GDPR and also makes some improvements as discussed in the following paragraphs.

III. Personal Data Protection Act 2018

In India the demand for a separate law for Privacy protection intensified with the initiative of the Government to use Aadhaar as an identity instrument for many of the activities of the Government including an attempt to link Bank accounts, PAN and property dealings with Aadhaar.

The Government formed an expert committee under the Chairmanship of Justice B.N Srikrishna, a retired Supreme Court judge which after an elaborate consultation process came up with a comprehensive report and a suggested a draft Bill titled "Personal Data Protection Act 2018" which was presented in the Parliament.

Since the term of the last parliament ended before it could be passed, the Bill has lapsed and is expected to be re-introduced in the next Parliament. However considering that the Bill would in all probability be passed more or less in the current form, we proceed to briefly discuss the provisions of the Bill in the following paragraphs. (Ed: Students may keep track of the changes that may occur in the Bill at www.pdpa2018.in).

PDPA 2018 largely follows the international principles set in GDPR but has its own few innovations which if properly recognized and brought into practice would make it a better legislation than GDPR.

If these innovations are not recognized in the general blindness created by the GDPR shadow, then precedents may set in creating wrong perceptions which may be difficult to remove.

The Structure of PDPA 2018

The PDPA 2018 has been divided into 15 chapters and two schedules.

Schedule I relates to the removal of Section 43A of ITA 2008 which will be replaced by the provisions of PDPA 2018. Schedule II relates to the amendments to the RTI Act.

Chapter XIV relates to the transitional provisions and the time schedule for the Act is fully implemented and Chapter XV relates to some miscellaneous provisions.

Chapter I contains the preliminary aspects including the definitions and Chapters II to XIII contain the other details of the Act.

Unlike GDPR, PDPA 2018 provides for criminal punishments under the Act under Chapter XIII which make it more stringent than the GDPR. The civil penalties are reasonably strong as it follows the GDPR model of fixing penalties for non compliance upto 4% of the global turnover of a company.

Chapter II deals with the Data Protection obligations and Chapters III to V prescribe the conditions under which personal/sensitive personal/children data may be processed.

Chapter VI indicates the specific rights of the Data Subject who is referred to as the "Data Principal" under the Act and Chapter VII indicate the compliance measures to be followed by the Data Processor and the Data Controller who is referred to as "Data Fiduciary" under the Act.

Chapter VIII sets the provisions regarding data transfer outside India and Chapter IX relates to exemptions.

Chapter XI indicates Penalties and Remedies followed by Chapter XII which provides details of the Appellate Tribunal to be constituted.

A full discussion of the PDPA 2018 is out of scope of this lesson and students may refer to the Book on PDPA and content available at www.privacy.ind.in .

Some of the key features of the Act are highlighted below.

The Concept of Data Fiduciary

One of the most innovative features of PDPA 2018 is that the Act does not define "Personal Data" as "Property" like the draft of DISHA did. But by using the term "Data Fiduciary" for the Data Controller and "Data Principal" for the Data Subject, the Act suggests that when personal data passes from the data subject to the data controller, the recipient assumes the role of a "Trustee" for the data and not as a "Controller" appointed by the data subject. The Data Principal remains the controller of the personal data but the recipient is appointed as a "Trustee". The establishment of the relationship is of "Fiduciary

nature" which means that the responsibilities of the fiduciary are presumed under the circumstances and need not be set in stone through a "Trust Deed".

The "Consent" which is the key to all data protection legislations does not assume the status of the "Trust Deed" but is only one of the many instruments or practices that may define the fiduciary relationship. It must be noted that under ITA 2000/8, a Trust deed cannot be created through an electronic document and hence an electronic consent cannot anyway assume the status of a trust deed. At best it can be a "Deemed" contract since in most cases it may not be digitally signed also.

A "Data Fiduciary", who collects the personal information and uses it himself or passes it onto a processor is expected to put in place such measures as to protect the "Privacy Rights" of the Data Principal.

The full import of this definition requires an in-depth debate and Cyber Jurisprudence will evolve in this respect over a period of time.

The provision however gives room to the establishment of Data Fiduciaries who act as only trustees of the data and supervise its distribution and use to the data processors. This would enable them to manage the difficulties of content fatigue which confronts data subjects. It will also enable professional data fiduciaries to act as a "Personal Data Repository", create different packages of personal data and share it with different data processors on a need to share basis.

These are concepts which are innovative in the global scenario that makes PDPA 2018 unique.

Data Principal's Rights

The rights of the data principal recognized under PDPA 2018 are similar to the rights recognized under GDPR and includes

1. Right to Confirmation and Access
2. Right to Correction
3. Right to Data Portability
4. Right to be forgotten

However, the Right to be forgotten under PDPA 2018 is subject to the "Adjudicator" approving the erasure. In comparison GDPR leaves it to the Data Controller to decide about the data erasure request and imposes penalty if there is an undue delay in executing the request of the data subject. This may lead to

deletion of data by an error. PDPA 2018 introduces a third party supervision before the data is deleted and this is essential to prevent wrongful erasure of data which could be evidence of crimes.

Registration of Fiduciaries

PDPA 2018 mandates that fiduciaries who process Sensitive personal information or large value of personal information (Significant Fiduciaries) and the personal information of Children (Guardian Fiduciaries) need to register themselves with the authority so that they can be monitored closely and also de-recognized if they are not compliant.

Data Audits and Data Trust Score

PDPA 2018 mandates annual Data Audits from an external agency which would be like the "Statutory Financial Audits" of companies.

It is also prescribed that such audits would use a "Data Trust Score" system[xii] to provide a measurability of the level of compliance like the Credit Scoring system prevalent in the financial markets.

Data Protection Officer

Under PDPA 2018 it is mandatory for a Data Fiduciary to designate a Data Protection Officer who is an employee of the organization. Under GDPR the DPO can be an external consultant but under PDPA 2018 it is not permitted. There is therefore a two level monitoring by an employee who is a Data Protection Officer and an external Data Auditor who reviews the system on an annual basis.

Data Localization

PDPA 2018 has prescribed that at least one serving copy of personal data collected under PDPA 2018 shall be kept in servers in India. In respect of Sensitive personal information, except under stated exemption clauses, data has to be mandatorily kept within India.

Data Protection Authority

For the regulation of PDPA 2018, a new authority called the Data Protection Authority (DPA) is set to be formed. It will consist of a Chairman and 6 members with representation from the industry. The functional regulation would be largely within the DPA who has to issue several compliance guidelines/codes of practice including the data breach notification norms, the data trust score systems, the data audit requirements etc.

The Adjudication system will work under the DPA but the DPA would be subject to the judicial supervision of an Appellate Tribunal which will be an external entity.

Staggered Implementation

In a departure from the past legislations in India. PDPA 2018 has adopted the concept of fixing a time line for implementation of the legislation. Accordingly after the passage of the Bill into an Act, activities such as notifying the date of effect, formation of the Data Protection Authority etc will be implemented.

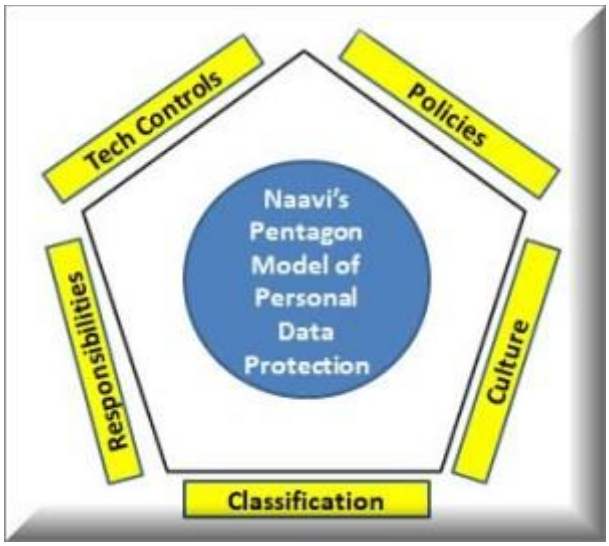
In summary it may be stated that the passage of PDPA 2018 which has already flowed over to 2019 will change the face of Data Protection regulation in India and would also have its impact on Cyber Laws in general in India.

Personal Data Protection Standard of India (PDPSI)

The PDPA 2018 has indicated that it would be one of the duties of the Data Protection Authority to specify codes of practice to promote good practices of data protection and facilitate compliance of the Act by the industry.

From the industry side, a framework has already been proposed for this purpose and is called the Personal Data Protection Standard of India (PDPSI).

PDPSI is a framework that adopts the Pentagon model of Personal Data Protection as depicted below.



Under this model, Five distinct categories under which the compliance efforts are directed namely

1. Appropriate Classification of Personal Data
2. Appropriate Responsibility distribution

3. Installing adequate and necessary Technical Controls
4. Adopting appropriate Policy Formulations
5. Developing a Culture of Privacy Protection

A gist of this standard is provided here.

1. **Objective:**

   The objective of PDPSI is to provide a standard that incorporates the known good practices embedded in other information security frameworks such as ISO 27001, BS10012, IISF-0309. As a standard, it would list the broad requirements of compliance and will be supported by "Implementation Specifications" which are more detailed.

   Within the broad scope of the "Standard", organizations would be free to adopt the implementation standards that come accredited with the standard as suggested annexures or implement modified methods subject to justification.

   The PDPSI takes into account the existing Data Protection law of India as contained in ITA 2000/8, the proposed PDPA 2018, the GDPR and HIPAA.

   PDPSI is meant for "Personal Data Protection" and hence would be distinct from the general Information Security Policy that the organization may have already adopted.

2. **Implementation Responsibility**

   PDPSI envisages that the Subject organization which could be a Data Fiduciary or Data Controller or a Data Processor, would constitute a Data Protection Committee which includes a member of the Board of Directors, the designated Data Protection Officer and other top management personnel relevant for compliance.

   It is recommended that the implementation responsibility is decentralized to the extent possible with a team of "Internal Data Controllers" assisting the DPO.

   The DPC will cause a Data Protection Impact Assessment to be conducted and develop a "Compliance Charter" which would be approved by the Board. To the extent the Board decides to adopt any deviation from the implementation specifications suggested under the PDPSI if any, the

Board will also approve the variance statement between the PDPSI implementation specification and the adopted implementation charter along with a documentation of the reasoning for approving the variance.

3. Data Classification

PDPSI is meant for protection of personal Data and as a first step, all personal data, namely data that contains an element of identity that can be linked to an individual, will be classified in such a manner that the applicable regulations can be identified with clarity to different sets of data that may be flowing into an organization.

4. Technical Controls

The technical controls are measures that the organization may adopt in the form of Firewalls, IDS, Anti Virus systems, Encryption systems, Access Control measures, Data Leak Prevention solutions, etc. Pseudonymization or De-identification is also a technical control that can be used to segregate data into “Protected Personal Data” and “No Need to be Protected Personal Data”.

5. Policy Controls

Policy Controls are the measures that are reflected in the written policies and procedures to which the organizational employees will be subject to and includes the Privacy Policy and the Personal Data Protection Policy along with other policies.

6. Culture of Privacy/Personal Data Protection

Measures to instill a culture of Privacy protection through Personal Data Protection includes all measures directed to people and to fine tune their behaviour towards compliance of Personal Data Protection regulation and internal guidelines.

Concluding Remarks

In this chapter we have tried to provide an overview of the development of “Data Protection” regulations in India. We have also discussed some of the emerging technology aspects and the challenges they pose. We have also discussed briefly there major privacy laws to indicate the general approach that such laws

take. In particular we have discussed the emerging Personal Data Protection law in India along with an industry framework for compliance namely the Personal Data Protection Standard of India.

This subject is fast developing and new regulations are emerging across the globe. Students may keep themselves updated with reference to the material available on the web some of which have been have been specifically indicated below.

References

1. http://www..information-assurance.com
2. https://www.naavi.org/wp/pentagon-model-of-personal-data-protection/
3. https://www.naavi.org/wp/hashing-the-547-pages-of-privacy-judgement/
4. http://ita2008.in/ita_2008/ch1_2008.htm
5. https://www.naavi.org/wp/section-65b-in-the-quantum-computing-scenario/
6. https://www.naavi.org/wp/section-65b-clarified-e-book/
7. https://www.naavi.org/wp/securing-the-world-against-rogue-robos/
8. https://en.wikipedia.org/wiki/Cambridge_Analytica
9. https://www.naavi.org/wp/legitimate-interest-policy/
10. http://disha2018.in/wp/
11. http://www.gdpr.ind.in/
12. https://www.naavi.org/wp/naavis-data-trust-score-model-unleashed-in-the-new-year/

Case References:

1. **CNIL Vs Google:** https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
2. **German District Court ruling under Art 82 GDPR:** https://newtech.law/en/first-compensation-for-gdpr-infringement/
3. **HIPAA cases and fines are detailed here:** https://www.hipaajournal.com/hipaa-violation-cases/

SUGGESTED READINGS

Articles:

1. N. S. Nappinai, Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study , 5 J. Int'l Com. L. & Tech. 22 2010

2. LEROY MCFARLANE , Forensic psychologist, Rampton Hospital, HMP Nottingham, and the Lucy Faithfull Foundation, CYBERSTALKING: THE TECHNOLOGY OF HATE, 76 Police J. 204 2003

3. MRINALINI SINGH & SHIVAM SINGH, CYBER CRIME CONVENTION AND TRANS BORDER CRIMINALITY, 1 Masaryk U. J.L. & Tech. 53 2007

4. "Cyber Laws in Information Age, Asia-Pacific Regional Workshop on Equal Access of Women in ICT Seoul, R.O. Korea, Oct. 22-26 2001",M. Ajmal Edappagath, Advocate, Supreme Court, India.

5. Major General Koen Gijsbers and Matthijs Veenendaal (MA), Protecting the National Interest in Cyberspace, 11 Geo. J. Int'l Aff. 191 2010-2011.

6. Melissa Hamilton, THE CHILD PORNOGRAPHY CRUSADE AND ITS NET-WIDENING EFFECT, 33 Cardozo L. Rev. 1679 2011-2012

7. Neel K Katyal, DEVELOPMENTS IN THE LAW THE JAW OF CYBERSPACE, 112 Harv. L. Rev. 1574 1998-1999.

8. Michael Edmund O'Neill, OLD CRIMES IN NEW BOTTLES: SANCTIONING CYBERCRIME, 9 Geo. Mason L. Rev. 237 2000-2001.

9. Dr. Rita Esen, Cyber Crime: A Growing Problem, 66 J. Crim. L. 269 2002.

Books

1. Patrick Hess, (ed.), *Cyber Terrorism and Information war*, 2002 ed., Anmol Publications Pvt. Ltd., New Delhi

2. Rahul Matthan, *The Law relating to Computers and the Internet*, 2000, Butterworths, New Delhi

3. SV Joga Rao, *Law of Cyber Crimes and Information Technology Law*, 2004 ed., Wadhwa and Company, Nagpur

4. Mark F. Grady and Francesco Parisi, (eds.), *The Law and Economics of Cyber security*, 2006, Cambridge University Press

5. P.M. Bakshi and R.K. Suri, (eds.), *Bharat's Handbook of Cyber and E-commerce laws*, 2002, Bharat Publishing House, New Delhi.

6. The Criminal Law Review Special Edition- *Crime, Criminal Justice and the Internet*, 1998, Sweet and Maxwell Ltd.

ANNEXURE

CASES ON CYBER CRIME

I. United States v. Jake Baker[139]

The case dealt with the posting of sexually explicit material by Abraham Jacob Alkhabaz, a student of the University of Michigan under the pseudonym "Jake Baker". Baker posted stories on an internet newsgroup titled "alt.sex.stories" describing the torture, rape and murder of a woman who had the same name as one of Baker's classmates at the University of Michigan. In addition, e-mails were exchanged between Baker and a man named Arthur Gonda from Ontario, Canada, who was a reader of his story. Over forty e-mails were exchanged between the two men discussing their desire to abduct and physically injure women of their area. As a result, a complaint was filed against Baker under the Interstate Communications Act.[140]

The District Court made a thorough analysis of the communications between Baker and Gonda to conclude that the case did not satisfy the "credible threat" standard. According to the Court, the statements of the defendant must meet the "unequivocal, unconditional, immediate and specific" standard, failing which the conduct in question cannot be penalized. Based on this standard the Court held that there was no specific class of target towards which the communications between the two men was directed, and the mere expression of desire to indulge in perverse acts was not sufficient to infer an intention to act in accordance with the desire.[141] In addition the Court also held that a class of women towards which these mails was directed was too vague and not sufficiently specific to meet the standards required to invoke penalty under the legislation.[142]

Therefore, it can be seen from this case that such grave offences which involve the use of specific names also do not amount to cyber-stalking under the current legal regime because they do not involve a "specific threat" towards the victim in question.

II. Manish Kathuria Case

The first reported case of cyber-stalking in India and the reason for the 2008 amendment to the IT Act,[143] the Manish Kathuria case involved the stalking of a woman named Ritu Kohli. Kathuria followed

---

139 890 F.Supp. 1375 (1995).
140 *Id*.
141 *Id*. at 1388.
142 *Id*. at 1389.
143 P. Shah, *Cyber Stalking & the Impact of its Legislative Provisions in India*, http://www.legalindia.in/cyber-stalking-the-impact-of-its-legislative-provisions-in-india (last visited Nov. 4, 2012).

Kohli on a chat website, abused her by using obscene language and then disseminated her telephone number to various people. Later, he began using Kohli's identity to chat on the website "www.mirc.com". As a result she started receiving almost forty obscene telephone calls at odd hours of the night over three consecutive days. This situation forced her to report the matter to the Delhi Police.[144] As soon as the complaint was made, Delhi Police traced the IP addresses and arrested Kathuria under Section 509 of the Indian Penal Code.[145] The IT Act was not invoked in the case, since it had not come into force at the time when the complaint was filed.

While there is no record of any subsequent proceeding, this case made Indian legislators wake up to the need for a legislation to address cyber-stalking. Even then, it was only in 2008 that Section 66-A was introduced. As a result, now cases are being reported under this section as opposed to Section 509 of the Indian Penal Code, as was the case where a Delhi University student was arrested for stalking a woman from Goa by creating fake profiles on social networking websites, uploading pictures on them and declared her to be his wife.[146] It is hoped that the decision in this would favour the victim. Verdict is yet to come.

III. Karan Girotra v. State[147]

The above case is the only reported case till date to reach the judiciary on cyber-stalking is also merely an application to grant anticipatory bail. The facts of the case are that Shivani Saxena, D/o Sudhir Saxena had lodged a complaint with the Police that she had married to Ishan on 25.9.2009, however, the marriage between them failed within a few days as her husband, Ishan could not consummate the marriage. Both of them started living separately w.e.f. 1.10.2009 and it was amicably settled between them that after the expiry of one year of their marriage, both of them will file a joint petition, on mutual consent, for the grant of divorce, after which both the parties will be free to marry afresh.

It is further alleged by her that in the course of chatting on the internet, she had come in contact with one Karan Girotra about six years back from the date of the lodging of the complaint. On 3.4.2010, the petitioner is alleged to have told her that he had fallen in love with her and wants to marry her. On this, she allegedly told him that she is already married, whereupon the petitioner said that he would marry her after her divorce. On 15.5.2010, it is alleged that on the pretext of introducing the complainant to his family members, the petitioner called her to his house, that is, Flat No. 11, Rama

---

144 D. Halder and K. Jaishankar, *Cyber Crimes against Women in India: Problems, Perspectives and Solutions*, 3(1) TMC ACAD. J. 48, 55 (2008).

145 Duggal, *supra* note 113.

146 N. Chauhan, DU Law Student Charged with Cyber Stalking, http://articles.timesofindia.indiatimes.com/2011-06-20/delhi/29679690_1_law-student-complaint-profiles (last visited Nov. 4, 2012).

147 Karan Girotra v. State, 2012 VAD (Delhi) 483.

Krishan Apartment, Sector-IX, Rohini, Delhi where she found that there was nobody except his old bed-ridden maternal grandmother. It is alleged by her that, at about 8:00 P.M., the petitioner gave her soft drink, which was perhaps laced with some intoxicant and on consuming the same, she became unconscious. It is stated that when she regained her consciousness at about 10:00 P.M., she found herself completely nude and she also noticed that she had been sexually assaulted. On noticing this, she started crying and she was consoled by the petitioner that she need not worry, as he would fulfill the commitment of marrying her. On 16.5.2010, she was shocked when she received her obscene pictures of the previous night. She confronted the petitioner with the said pictures, whereupon the petitioner represented to her that she need not worry about this and he is going to marry her. It has also been alleged that the petitioner threatened to circulate the objectionable pictures everywhere if she did not keep on maintaining physical relations with him. On the basis of this blackmail, she alleged that she was raped again on 18.5.2010. Subsequent thereto, on 9.7.2010, it is stated that a roka ceremony was held between the petitioner and the complainant at the restaurant, Pind Baluchi in Pitam Pura, Delhi, where the mother of the complainant gifted the petitioner a santro car, jewellery, clothes and various other gift items. It has been alleged that the petitioner kept on sexually assaulting the complainant without her consent and on 12.9.2010, the petitioner informed the complainant's mother that he is breaking the engagement and he returned the car and the other articles, whereupon the complainant lodged a complaint in the month of June and the aforesaid FIR under Sections 328/376 IPC read with Section 66A of the I.T. Act was registered by PS: Prashant Vihar, Delhi against the petitioner. As a result, Saxena filed a complaint under Section 66-A of the IT Act.

Though the Court rejected the plea of anticipatory bail on the ground that nude and obscene pictures of Saxena were circulated by Girotra, an act which requires serious custodial interrogation, nonetheless it made some scathing remarks. According to the Court Saxena had failed to disclose her previous marriage to Girotra merely because she agreed to perform the engagement ceremony, even though such mention was made when Girotra had first professed his love to Saxena.[148] The Court also took noted that there was a delay in lodging the FIR by Saxena. What is more shocking is that the Court held that Saxena had consented to the sexual intercourse and had decided to file the complaint only when Girotra refused to marry her.[149]

This case highlights the attitude of the Indian judiciary towards cases involving cyber-stalking. It is appalling that factors as redundant as a delay in filing the FIR have a huge bearing on the outcome of the case. It is for this reason that more stringent legislations are the need of the hour.

[148] *Id*.
[149] *Id*.

IV. YAHOO! Inc. v. LICRA

169 F. SUPP. 2d 1181 (N.D.Cal.2001)

Defendants La Ligue Contre Le Racisme Et l'Antisemitisme ("LICRA") and L'Union Des Etudiants Juifs De France, citizens of France, are non-profit organizations dedicated to eliminating anti-Semitism. "Yahoo!" is a corporation organized under the laws of Delaware with its principal place of business in Santa Clara, California. Yahoo! is an Internet service provider that operates various Internet websites and services that any computer user can access at the Uniform Resource Locator (" URL") http:// www. yahoo.com. Yahoo! services ending in the suffix, ".com," without an associated country code as a prefix or extension (collectively, "Yahoo!'s U. S. Services") use the English language and target users who are residents of, utilize servers based in and operate under the laws of the United States. Yahoo! subsidiary corporations operate regional Yahoo! sites and services in twenty other nations. Yahoo!'s regional sites use the local region's primary language, target the local citizenry, and operate under local laws[150].

Yahoo! provides a variety of means by which people from all over the world can communicate and interact with one another over the Internet. Examples include an Internet search engine, e-mail, an automated auction site, personal web page hostings, shopping services, chat rooms, and a listing of clubs that individuals can create or join. Any 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. As relevant here, 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 party 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.

[150] http://www.tomwbell.com/NetLaw/Ch03/YahoovLICRA.html.

On or about April 5, 2000, 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 violates French law. LICRA threatened to take legal action unless Yahoo! took steps to prevent such sales within eight days. Defendants subsequently utilized the United States Marshal's Office to serve Yahoo! with process in California and filed a civil complaint against Yahoo! in the Tribunal de Grande Instance de Paris (the "French Court").

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 exhibition of Nazi propaganda and artifacts for sale.n2 On May 20, 2000, the French Court entered an order-requiring Yahoo! to (1) eliminate French citizens' access to any material on the Yahoo.com auction site that offers for sale any Nazi objects, relics, insignia, emblems, and flags; (2) eliminate French citizens' access to web pages on Yahoo.com displaying text, extracts, or quotations from *Mein Kampf and Protocol of the Elders of Zion;* (3) post a warning to French citizens on Yahoo.fr that any search through Yahoo.com may lead to sites containing material prohibited by Section R645-1 of the French Criminal Code, and that such viewing of the prohibited material may result in legal action against the Internet user; (4) remove from all browser directories accessible in the French Republic index headings entitled "Zionists" and from all hypertext links the equation of "Zionists" under the heading "Holocaust." The order subjects Yahoo! to a penalty of 100,000 Euros for each day that it fails to comply with the order.

Any item that promotes, glorifies, or is directly associated with groups or individuals known principally for hateful or violent positions or acts, such as Nazis or the Ku Klux Klan. Official government-issue stamps and coins are not prohibited under this policy. Expressive media, such as books and films, may be subject to more permissive standards as determined by Yahoo! in its sole discretion.

What *is* at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation. In a world in which ideas and information transcend borders and the Internet in particular renders the physical distance between speaker and audience virtually meaningless, the implications of this question go far beyond the facts of this case. The modern world is home to widely varied cultures with radically divergent value systems. There is little

doubt that Internet users in the United States routinely engage in speech that violates, for example, China's laws against religious expression, the laws of various nations against advocacy of gender equality or homosexuality, or even the United Kingdom's restrictions on freedom of the press. If the government or another party in one of these sovereign nations were to seek enforcement of such laws against Yahoo! or another U. S.-based Internet service provider, what principles should guide the court's analysis?

The Court has stated that it must and will decide this case in accordance with the Constitution and laws of the United States. It recognizes that in so doing, it necessarily adopts certain value judgments embedded in those enactments, including the fundamental judgment expressed in the First Amendment that it is preferable to permit the non-violent expression of offensive viewpoints rather than to impose viewpoint-based governmental regulation upon speech. The government and people of France have made a different judgment based upon their own experience. In undertaking its inquiry as to the proper application of the laws of the United States, the Court intends no disrespect for that judgment or for the experience that has informed it.

LEGAL ISSUES

In the present case, the French court has determined that Yahoo!'s auction site and website hostings on Yahoo.com violate French law. Nothing in Yahoo!'s suit for declaratory relief in this Court appears to be an attempt to re-litigate or disturb the French court's application of French law or its orders with respect to Yahoo!'s conduct in France. Rather, the purpose of the present action is to determine whether a United States court may enforce the French order without running afoul of the First Amendment. The actions involve distinct legal issues, and as this Court concluded in its jurisdictional order, a United States court is best situated to determine the application of the United States Constitution to the facts presented. No basis for abstention has been established. What makes this case uniquely challenging is that the Internet in effect allows one to speak in more than one place at the same time. Although 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.

V. AVINASH BAJAJ V. STATE OF DELHI[151]

Avinash Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website, a video clip was offered for sale, shot on a mobile phone of two children of a school in Delhi indulging in an explicitly sexual act. The managing director was prosecuted under sec

[151] (2005) 3 CompLJ 364 (Del)

292 and sec 67 of the act. He contended that bazee.com is only a service provider and provides a platform and when it has come to his notice it was withdrawn immediately. This is the first case registered under sec 67 and still proceedings in the court are going on. MD is enlarged on mobile. The Supreme Court in an interim order said “The question for the purposes of Section 67 is whether the website caused the publishing of such obscene material. For this purpose, the chain of transactions is relevant. Once the interested buyer gets on to baazee.com and views the listing, he then opts to buy the said product and then makes payment. Only then the remaining part of the chain is complete and the product, which in this case is the video clip in electronic form, is then transmitted through an email attachment and then can get further transmitted from one person to another. The video clip sent as an email attachment can straightway be downloaded onto to the buyer's hard disc and numerous copies thereof can be made for further transmission. The 'publishing' in this form is therefore instantaneous and can be repeated manifold. In fact in the present case, the transmission of the clip to eight buyers located in different parts of the country took place in a very short span of time.

Therefore, it cannot be said that baazee.com in this case did not even prima facie "cause" the publication of the obscene material. The ultimate transmission of the video clip might be through the seller to the buyer but in a fully automated system that limb of the transaction cannot take place unless all the previous steps of registration with the website and making payment take place. It is a continuous chain. When five to six links of the chain are under the direct control of the website and it is only on completion of each step that the final two steps which result in the actual publication of the obscene material ensue, it cannot be said that the website did not even prima facie cause publication of the obscene material.

The user agreement, downloaded from the site and details seized from, Sharat Digumarti, indicates that arrangements arrived at between buyers and sellers are bipartite agreements with no responsibility of Baazee.com whatsoever. However, in this case Baazee.com acted as an agent of the seller as it had taken a commission on the sale. The clip was priced at Rs.125/- each, but billed at Rs.128/- each with Rs.3/- as commission per sale. This commission was credited to Paisa Pay, a division of Baazee.com. The website Baazee.com had installed a program which runs SQL crawl jobs or checks the written words place by the sellers against a set of banned and suspect words. The web portal is a public domain and can be accessed and read by just anyone. The language of the advertisement placed on the website was quite explicit and left nothing for the reader to imagine. The website was committed to block off offending words through appropriate filters, as per Clause 1.12.4 Schedule 'C' Part II: Terms & Conditions of the ISP guidelines, issued by the Government of India, which clearly states therein that "The Licensee shall ensure that objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, Intellectual Property right and International and domestic Cyber Laws, in any form or inconsistent with the laws of India, are not carried in his network, the ISP should

take all necessary measures to prevent it." However, in-spite of the filters having the word 'sexual' in its list, the program of Baazee.com failed to block off the offending advertisement. Further, in-spite of being categorically informed by one of the users' thread sincp@sify.com on 27.11.2004 at 8.20 p.m. the company, Baazee.com a 24 x 7 platform, failed to act to stop the sale, immediately. All through the day on 28.11.2004 the sale was going on unabated and it was finally closed on 29.11.04.

After having gathered enough evidences to establish that the porn video film was listed for sale, that it was actually purchased by at least 8 buyers, that the clipping was delivered to 8 buyers as email attachment through Baazee.com, that payments were passed on to the accused Ravi Raj col. No. 4., after deducting due commissions, that in spite of being categorically informed by one of the users thread sincp@sify.com on 27.11.04 at 8.20 P.M. Baazee.com failed to act to stop the sale, immediately, but closed it only after 38 hours, accused Avinash Bajaj, CEO of Baazee.com mentioned in Col. No. 4 was arrested on 17.12.04"

The Information Technology Act of 2000 was enacted with an aim to recognize electronic records and facilitation of e-commerce.[152] To this extent, hardly ten sections were incorporated that actually dealt with cybercrime. One of these was Section 67, which dealt with the publishing or transmitting of pornographic material through a computer resource.[153] It did not consider the need for specialized provisions regarding child pornography. However, it is pertinent to note that this Act was a significant step forward from the existing law. Under the Indian Penal Code, 1860, the Indian Post Office Act, 1898 and the Indecent Representation of Women (Prohibition) Act, 1986, only obscene visual representations were the focus of the legislation. It left out audio materials and simulated images both of which are recognized internationally.[154] As far as Indian constitutional jurisprudence is concerned, obscenity is not a protected expression under Article 19(1) (a), and thus can be validly restricted under Article 19(2) on the ground of decency or morality.[155] When obscenity is judged as per the proper tests, and is deemed to be obscene by the court, there can be no allegation of a violation of Article 19(1) (a). It is in this pursuance of removing the obscene material from the website that the site is blocked under the IT Act. Prohibition is

---

[152] Nappinai, Cyber crime in India: Has law kept pace with emerging trends? An empirical study, JICLT VOL.5, ISSUE 1 (2010) 1.

[153] Section 67. Punishment for publishing or transmitting obscene material in electronic form – Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[154] Ecpat Network Feedback on progress since World Congress III available at Wc%20iii_follow_up_inputs_Ei_Groups.Pdf (Last Accessed September 18, 2011).

[155] *K.K. Kochuni*v. *State of Madras*, AIR 1960 SC 1080

merely a form of restriction of a fundamental right.[156] As such, the object of the block is to prevent users Internet from accessing that material. As shown through the earlier case of *Center for Democracy & Technology* v. *Pappert,*[157] this is can be only inadequately accomplished.

VI. Delhi Balbharathi Case:

In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face.

He decided to take revenge on his tormentors. He created a website at the URL www.amazing-gents.8m.net. The website was hosted by him on free web space. It was dedicated to Air Force Balbharti School and contained text material. On this site, lucid, explicit, sexual details were given about various "sexy" girls and teachers of the school. Girls and teachers were also classified on the basis of their physical attributes and perceived sexual preferences. The website also became an adult boys' joke amongst students.

This continued for sometime till one day, one of the boys told a girl, "featured" on the site, about it. The father of the girl, being an Air Force officer, registered a case under section 67 of the IT Act, 2000 with the Delhi Police Cyber Crime Cell.

Police picked up the concerned student and kept him at Timarpur (Delhi) juvenile home. It was almost after one week that the juvenile board granted bail to the 16- year-old student.[158] This case is under investigation.

---

[156] *Narendra Kumar* v. *Union of India*, (1960) 2 S.C.R. 375; *Chintaman Rao* v. *State of Madhya Pradesh*, AIR 1951 SC 118, *Cooverjee B. Baruchav. Excise Commr. And the Chief Commr., Ajmer*, (1954) S.C.R. 873; *M.B. Cotton Association Ltd.* v *.Union of India*, ('54) A.SC. 634.

[157] 337 F. Supp. 2d 606, 642, 650, 655 (E.D. Pa. 2004).

[158] http://www.indiaforensic.com/compcrime1.htm.

Refer: www.information-assurance.com
https://www.naavi.org/wp/pentagon-model-of-personal-data-protection/
https://www.naavi.org/wp/hashing-the-547-pages-of-privacy-judgement/
http://ita2008.in/ita_2008/ch1_2008.htm
https://www.naavi.org/wp/section-65b-in-the-quantum-computing-scenario/
https://www.naavi.org/wp/section-65b-clarified-e-book/
https://www.naavi.org/wp/securing-the-world-against-rogue-robos/
https://en.wikipedia.org/wiki/Cambridge_Analytica
https://www.naavi.org/wp/legitimate-interest-policy/
http://disha2018.in/wp/
http://www.gdpr.ind.in/
https://www.naavi.org/wp/naavis-data-trust-score-model-unleashed-in-the-new-year/