UNIT–1

Introduction to Cyber Crimes

Notes

(Structure)

Notes

1.1 Learning Objectives

After studying the chapter, students will be able to:

- Discuss the Cyber crime and cyber Law;
- Explain the Cyber Crime and Origin of Cyber Crime;
- Discuss the Jurisprudence of Indian Cyber Law and Crime;

Notes

- Describe the Cyber Crimes and Conventional Crimes;
- Discuss the Distinction between Conventional & Cyber Crime;
- Describe the Classification of Cyber Crime;
- Explain the technology in cyber crime;
- Describe the Provisions Information Technology Act in Protection of Cyber crime;
- Discuss the Categories of Cyber Crimes;
- Describe the Distinction between Individual, Property, Government Cyber Crime;
- Explain the Cyber Crime;
- Discuss the Tackle Cyber Crime;
- Explain the Computer Forensics;
- Discuss the objectives of Computer Forensics;
- Explain the Cyber Forensics;
- Describe the Misuse of computer forensics;
- Explain the provisions of Indian Evidence Act, 1872?
- Explain the Digital Evidence and law dealing;
- Discuss the Computer Forensics;
- Explain the flaws in its Current Scenario;
- Discuss the misuse of cyber forensics and investigation.

1.2 Introduction

"Cyberspace" is a very wider term. Most of us have a limited knowledge of "Cyberspace" and the crimes occurring in "cyberspace", known as cybercrime, which happens on computer and the Internet, however, cybercrime has a severe potential for remarkable impact on the lives of individuals and our society. Therefore, a detailed introduction of cybercrime needs to be understood. There are many terms used to describe cybercrime. The former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime and Other forms include "digital", "electronic", "virtual", "IT", "High-tech" and Technology-enabled" crime. However, on the one hand, each of them didn't cover the whole meaning of cybercrime, because there is no incorporation of networks. On the other hand, terms such as "high-tech" or "electronic" crime might be too broad to specify that the crime is the exact

Notes

cybercrime, since other fields also have "hi-tech" developments like nanotechnology and bioengineering. Currently, although no one term has become totally dominant in use, "cybercrime" is the term used most pervasively. In general, cybercrime has three categories:

1. **Target cybercrime:** The crime in which a computer is the target of the offense.
2. **Tool cybercrime:** The crime in which a computer is used as a tool in committing the offense.
3. **Computer incidental:** The crime in which a computer plays a minor role in committing the offense.

The history of cybercrime is short compared with traditional crimes. The first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment allowed them to access into mainframe computers. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because of no Internet in that era. In following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. Since Internet was invented, people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental. This process is similar to the process of learning one language. In childhood, we learn language itself; then, when we grow up and are good at it, we will use it to communicate with each other but itself is not a prime element. In general, current consensus on the classification of cybercrime is to divide it into three categories that are said in the first paragraph above. We can set another analogy: target cybercrime is like crossword, which focuses on the magic of language itself; tool cybercrime is similar to fraud or harassment on street or in other face-to-face ways, but the place in which tool cybercrime happens is not physical environment but cyberspace; computer incidental including some electronic proof is saved in computer or the camera captures the criminal withdrawing money in a bank. Generally, these three categories are elaborated in the three following sections and in each section some latest cases will be studied.

Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace". Thus, it is necessary to introduce cybercrime detailed. While there are several textbooks talking about cybercrime, but focusing on

Notes

the statutes and laws relevant this new breed of crime, few papers or textbooks focus on the "computer science" itself. In other words, most of materials talk about the "crime" of "cybercrime", but this paper will talk more about "cyber".

The term ―cybercrime is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cybercrime 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.

Before evaluating the concept of cybercrime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

The history of cybercrime is short compared with traditional crimes. The first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment allowed them to access into mainframe computers. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because of no Internet in that era.

At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental. This process is similar to the process of learning one language. In childhood, we learn language itself; then, when we grow up and are good at it, we will use it to communicate with each other but itself is not a prime element. In general, current consensus on the classification of cybercrime is to divide it into three categories that are said in the first paragraph above. We can set another analogy: target cybercrime is like crossword, which focuses on the magic of language itself; tool cybercrime is similar to fraud or harassment on street or in other face-to-face ways, but the place in which tool cybercrime happens is not physical environment but cyberspace; computer incidental including some electronic proof is saved in computer or the camera captures the criminal withdrawing money in a bank. Generally, these three categories are elaborated in the three following sections and in each section some latest cases will be studied.

Technology has taken the world by storm in recent decades; the advent of the computer has completely revolutionized the way people live, work and play. Particularly, computers have affected businesses in numerous ways, allowing them to run more efficiently. However, there is a dark side to computers, when individuals use them to lash out malicious assaults. These assaults may include fraud, identity theft, hacking, embezzlement and a wide array of other activities. When these individuals are caught,

specialists are called in to seize and gather information from the computers. Computer forensics is the science of locating; extracting, analyzing and protecting types of data from different devices, which specialists then interpret to serve as legal evidence.

Notes

Computer crimes have been occurring for nearly 30 years, since computers were being used in production. Evidence can be derived from computers and then used in court. Initially, judges accepted the computer-derived evidence as no different from other forms of evidence; however, as data became more ambiguous with the advancement of computers, they were not as reliable.

Computers have become an important part of our lives and as such are involved in almost everything we do from paying bills to booking vacations. However, computer systems have also become the mainstay of criminal activity. And when the individuals involved are brought before the courts, innocence or guilt is basically decided by testimonies and evidence. Of the two areas, evidence is probably the area most key. And when it comes to evidence it is the accuracy of that evidence which may be the difference in determining the outcome of the trail. Relying more and more on the evidence extracted from computer systems to bring about convictions has forged a new means of scientific investigation. The term used to coin this area of investigation is computer forensics. It is an area of science that has come under the scrutiny of law enforcement, federal, state, and local government officials. And the reason for the scrutiny revolves around the cleanliness' of the data being presented.

Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. The three main steps in any computer forensic investigation are acquiring, authenticating, and analyzing of the data. Acquiring the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the ensuring that the copy used to perform the investigation is an exact replica of the contents of the original hard drive by comparing the check sums of the copy and the original. Analysis of the data is the most important part of the investigation since this is where incriminating evidence may be found.

Part of the analysis process is spent in the recovery of deleted files. The job of the investigator is to know where to find the remnants of these files and interpret the results. Any file data and file attributes found may yield valuable clues. Investigation of Windows and UNIX systems are similar in some ways, but the forensic analyst can tailor the investigation to one or the other since each operating system is different in unique ways. If deleted data could not be recovered through the use of common forensic tools, more sensitive instruments can be used to extract the data, but this is rarely done because of the high cost of the instruments. Data recovery is only one aspect of the forensics investigation. Tracking the hacking activities within a compromised system

is also important. With any system that is connected to the Internet, hacker attacks are as certain as death and taxes. Although it is impossible to completely defend against all attacks, as soon as a hacker successfully breaks into a computer system the hacker begins to leave a trail of clues and evidence that can be used to piece together what has been done and sometimes can even be used to follow a hacker home. Computer forensics can be employed on a compromised system to find out exactly how a hacker got into the system, which parts of the system were damaged or modified. However, system administrators must first be educated in the procedures and methods of forensic investigation if a system is to be recovered and protected. With the help of computer forensics, administrators are able to learn about mistakes made in the past and help prevent incidents from occurring in the future.

Each time any kind of input is fed into the computer, whether it is a key pressed on your keyboard, or a click on the mouse, a signal is generated and sent to the appropriate computer application and they can be intercepted in your computer via a software program that is running in the background or physically from some external device.

Keystroke loggers are made specifically for this purpose and can be employed by a network administrator to ensure employees are not misusing the company resources; or they can be used by hackers to steal passwords, social security numbers, and any other sensitive information entered by an unsuspecting person. Because of the wealth of information that can be gained from a computer forensics investigation, ethical considerations should be examined. Computer forensics is essentially a means for gathering electronic evidence during an investigation. In order to use this information to prosecute a criminal act and to avoid suppression during trial, evidence must be collected carefully and legally. It is particularly important to be aware of the privacy rights of suspects, victims and uninvolved third parties. An investigator needs to have knowledge of several laws and statutes that govern electronic evidence collection including the fourth amendment of the constitution, 18 U.S.C. ß2510-22, also known as the wiretap statute, the Electronic Communications Privacy Act (ECPA), and the USA PATRIOT Act. Each of these items affects the legality of electronic evidence and the appropriate procedures to acquire that evidence.

The general laws in India were drafted and enacted in the 19th century. Whilst each of the general laws have undergone modifications and amendments, the broad and underlying provisions have withstood the test of time, including unimaginable advancements in technology, which speaks to the dynamism of the General laws. The general laws referred to in this Article 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).

Notes

India got its first codified Act in the Information Technology Act, 2000 (IT Act), which fell far short of the Industry's requirements to meet global standards. The focus if the IT Act was however recognition of electronic records and facilitation of e-commerce. Barely ten sections were incorporated in the IT Act to deal with Cyber Crime.

At the time when the IT Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks, data theft, illegal access to data / accessing and removal of data without the consent of the owner, etc., were listed as civil penalties under the IT Act. The IT Industry continued to rely on self –regulation and contractual undertakings to appease its global clients, as it had done before the passing of the IT Act. The primary offences under the IT Act were:

- Tampering with source code;
- Deleting, destroying or altering any data on any computer resource with mala fide intent to cause wrongful loss or to diminish its value;
- Publishing or transmitting pornographic material through a computer resource;
- Provisions pertaining to encryption technology, the right of the Government authorities to intercept and decrypt such data and to call upon any entity or individual to decrypt such data were also included in the IT Act. Certain acts affecting the integrity and sovereignty of the nation were classified as offences.

In the era of 21st century which is going more advances and developing day by day, where technologies promote themselves with a rapid rate, which attracts human mind as it is much suitable for them in their busy & hectic schedule. However, all new technologies are less time consuming and much beneficial for human point of view.

Since, 21st century is much popular in itself which is stick in every human mind as it is an era which is now known for the upcoming war i.e., termed as cyber war where the fight is not between arms and explosives but it occurs between computers/laptops or any electronic gadget which consists of web application in it. However, security is much important area for each and every organization or any firms which consists of personnel information of any individual. The challenges in such cases are not only technological, but also jurisdictional. Many countries are involving itself to combating the cybercrime by implementing laws and acts, while India is a country which implement their jurisdictional problems by implementing Information Technology Act, 2000 (Amended 2008) with certain guidelines, various laws for cybercrime with its objective.

The issues which are arising with Indian Government are that many of its government officials didn't know how to investigate cybercrimes. However, this is not the problem of Indian government but many other countries facing the same problem

with their officials. To conflict with this issue government have to promote some officials who are experts and consists of a sound or good knowledge of cybercrimes, solution for it and also last but not least an official also consists of a fine knowledge of cyber laws and its implementation. For which they firstly have to know about search and seizure of digital evidence and after that they should get aware of how to preserve these evidences.

1.3 Origin of Cyber Crime

It is believed the first recorded cybercrime took place in the year 1820. This can be true with the fact that, computer did exist since 3500 BC in India, China and Japan. The modern computer began with the analytical engine of Charles Babbage.

Banks and other financial institutions were amongst the first large scale computer users in the private sector, for automate payroll and accounting functions. Therefore, fraud in a computer scheme merged. One of the first cases cited as an instance of the computer fraud involved equity-funding Corporation in the US, fraud was simple. The frauds succeed because the auditors and regulators accepted computer printouts as definitive evidence of policies and did not ask original documentation. When the fraud was discovered, some 64,000 out of 97,000 policies allegedly issued by the company proved to be false, almost 1 Billion pounds estimated to be the loss.

Therefore as the technological advance, the number of cybercrime cases increased. There is no reliable and precise statistics of the losses the victims gain as the fact that victims do not detect many of these crimes. Therefore, fights against computer crime began. Several individuals were engaged in the fight against computer crime from the early development. The founder and father of the knowledge of computer crimes are by many observers considered to be Donn B. Parker, USA. He was involved in the research of computer crime and security from the early 1970. He served as a Senior Computer Security Consultant at the SRI International (Stanford Research Institute), and was the main author of the first basic federal manual for law enforcement in the USA: Computer Crime –Criminal

Justice Resource Manual (1979). This manual became so on an encyclopedia also for law enforcement outside US.

1.4 What is Cyber Law?

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices.

(Such as hard disks, USB disks etc.), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Law encompasses the rules of conduct:

1. That have been approved by the government, and
2. Which are in force over a certain territory, and
3. Which must be obeyed by all persons on that territory?

Notes

Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Cybercrimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cybercrime. Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity.

The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

These include:

- Copyright law in relation to computer software, computer source code, websites, cell phone content etc.
- Software and source code licenses
- Trademark law with relation to domain names, Meta tags, mirroring, framing, linking etc.
- Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,
- Patent law in relation to computer hardware and software.

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

1.5 Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.
3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.
5. Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
6. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
7. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.
8. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the original' information, so to say, remains in the possession' of the owner' and yet information gets stolen.

1.6 Jurisprudence of Indian Cyber Law

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic

Notes

records with the Government. The IT Act also penalizes various cybercrimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to ′ 1 crore).

An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate. Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002. The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government.

It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA.

These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July

2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002. The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000.

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT. Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to

adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers. The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23rd March 2003 appointing the Secretary of Department of Information Technology of each of the States or of Union Territories' of India as the adjudicating officers. The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.

An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website. The Indian Penal Code (as amended by the IT Act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act).

In case of bank records, the provisions of the Bankers Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cybercrimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

The Reserve Bank of India Act was also amended by the IT Act.

1.7 Introduction to Cyber Crime

The first recorded cybercrime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

Notes

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage ego discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.

Today computers have come a long way, with neural networks and Nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather sinister implications. Major Cybercrimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised 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. He was finally arrested on Heathrow airport on his way to Switzerland.

1.8 Defining Cyber Crime

At the onset, let us satisfactorily define “cybercrime” and differentiate it from “conventional Crime”. Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Defining cybercrimes, as “acts that are punishable by the Information Technology Act” would be unsuitable as the Indian Penal Code also covers many cybercrimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cybercrime would be “unlawful acts wherein the computer is either a tool or a target or both”.

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

Financial crimes: This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands

of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

Cyber Pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc.). Recent Indian incidents revolving around cyber pornography include the Air Force Bal bharati School case. A student of the Air Force Bal bharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at history mentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai police arrested the couple for pornography.

Sale of Illegal Articles

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling: There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes: These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Email Spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails,

Notes

purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

Cyber Defamation

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

In a recent occurrence, Surekha (names of people have been changed), a young girl was about to be married to Suraj. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant. Then, one day when she met Suraj, he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about Surekha's character. Some of them spoke of affairs, which she had in the past. He told her that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, Suraj was able to prevail upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails.

During investigation, it was revealed that the person sending those e-mails was none other than Surekha's stepfather. He had sent these e-mails so as to break up the marriage. The girl's marriage would have caused him to lose control of her property of which he was the guardian till she got married.

Another famous case of cyber defamation occurred in America. All friends and relatives of a lady were beset with obscene e-mail messages appearing to originate from her account. These mails were giving the lady in question a bad name among her friends. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing they had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene e-mails they

also put up websites about her, that basically maligned her character and sent e-mails to her family and friends containing matter defaming her.

Cyber Stalking

Notes

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

1.9 Frequently Used Cyber Crimes

Unauthorized access to Computer Systems or Networks

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking".

Theft of information contained in electronic form

This includes information stored in computer hard disks, removable storage media etc.

Email Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the schemes were available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data Diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

Salami Attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small

Notes

amount of money (say ′ 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month. To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems. Logic bombs are programmes, which are activated on the occurrence of a particular predefined event. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.

Denial of Service Attack

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

Virus/worm Attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up the entire available space on a computer's memory. The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus beat the Melissa virus hollow – it became the world's most prevalent virus. It struck one in every five personal computers in the world.

When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10billion.

The original VBS_LOVELETTER utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE- LETTER-FORYOU. TXT. vbs". The subject line and those who had some knowledge of viruses did not notice the tiny .vbs extension and believed the file to be a text file conquered people wary of opening e-mail attachments. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Since, the initial outbreak over thirty variants of the virus have been developed many of them following the original by just a few weeks. In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user. Unlike the Melissa virus this virus does have a destructive effect. Whereas the Melissa, once installed, merely inserts some text into the affected documents at a particular instant during the day, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever- increasing versions of itself. Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

Logic Bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan Attacks

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

There are many simple ways of installing a Trojan in someone's computer. To cite and example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the 14th of February, he sent Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the

Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

Notes

Internet Time Thefts

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In a case reported before the enactment of the Information Technology Act, 2000 Colonel Bajwa, a resident of New Delhi, asked a nearby net café owner to come and set up his Internet connection. For this purpose, the net café owner needed to know his username and password. After having set up the connection he went away with knowing the present username and password. He then sold this information to another net café. One week later Colonel Bajwa found that his Internet hours were almost over. Out of the 100 hours that he had bought, 94hours had been used up within the span of that week. Surprised, he reported the incident to the Delhi police. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested the net café owner under the charge of theft as defined by the Indian Penal Code. The net café owner spent several weeks locked up in Tihar jail before being granted bail.

Web Jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website. In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled ‘How to have fun with goldfish’. In all the places where it had been mentioned, they had replaced the word ‘goldfish’ with the word ‘piranhas’. Piranhas are tiny but extremely dangerous flesh – eating fish.

Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

Theft of Computer System

This type of offence involves the theft of a computer, some part(s) of a computer or peripheral attached to the computer.

Physically Damaging a Computer System

This crime is committed by physically damaging a computer or its peripherals. Rehabilitation

1.10 Misuse of Technology

The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyze etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cybercrimes at the domestic and international level as well.

1.11 Conventional Crime

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is a legal wrong that can be followed by criminal proceedings which may result into punishment. 'The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences'. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

1.12 Cyber Crime

Cybercrime is the latest and perhaps the most complicated problem in the cyber world. Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime.

A generalized definition of cybercrime may be unlawful acts wherein the computer is either a tool or target or both' The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized

Notes

access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

1.13 Distinction between Conventional & Cyber Crime

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exist a fine line of demarcation between the conventional and cybercrime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium.

1.14 Reasons for Cyber Crime

Hart in his work The Concept of Law' has said ―human beings are vulnerable so rule of law is required to protect them. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cybercrime. The reasons for the vulnerability of computers may be said to be:

1. **Capacity to store data in comparatively small space:** The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.
2. **Easy to access :** The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
3. **Complex :** The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
4. **Negligence :** Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cybercriminal to gain access and control over the computer system.
5. **Loss of evidence :** Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyzes this system of crime investigation.

1.15 Cyber Criminals

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals.

1. **Children and adolescents between the age group of 6 – 18 years:** The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.
2. **Organised hackers:** These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.
3. **Professional hackers / crackers:** Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.
4. **Discontented employees : This group include those people who have been** either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

1.16 Mode and Methods of Committing Cyber Crimes

1. **Unauthorized access to computer systems or networks / Hacking:** This kind of offence is normally referred as hacking in the generic sense. However the framers of the Information Technology Act, 2000 have nowhere used this term so to avoid any confusion we would not interchangeably use the word hacking for ―unauthorized access as the latter has wide connotation.
2. **Theft of information contained in electronic form:** This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.
3. **Email bombing:** This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

Notes

4. **Data diddling:** This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerized.
5. **Salami attacks:** This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. The Ziegler case, where a logic bomb was introduced in the bank system, which deducted 10 cents from every account and deposited it in a particular account.
6. **Denial of Service attack:** The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.
7. **Virus / worm attacks:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988.
8. **Logic bombs:** These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).
9. **Trojan attacks:** This term has its origin in the word ―Trojan horse. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is through e-mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cybercriminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.
10. **Internet time thefts:** Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa's case- the Internet hours were used

up by any other person. This was perhaps one of the first reported cases related to cybercrime in India. However this case made the police infamous as to their lack of understanding of the nature of cybercrime.

11. **Web jacking:** This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the—gold fish case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded a ransom. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

1.17 Motive Behind Any Attack

1. Putting the public or any section of the public in fear; or
2. Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or
3. Coercing or overawing the government established by law; or
4. Endangering the sovereignty and integrity of the nation.

1.18 Classification of Cyber Crime

The subject of cybercrime may be broadly classified under the following three groups. They are:

1. **Against Individuals**
   (i) Their person &
   (ii) Their property of an individual
2. **Against Organization**
   (i) Government
   (ii) Firm, Company, Group of Individuals.
3. **Against Society at large**

The following are the crimes, which can be committed against the following groups

Against Individuals:

(i) Harassment via e-mails.

(ii) Cyber-stalking.

Notes

(iii) Dissemination of obscene material.

(iv) Defamation.

(v) Unauthorized control/access over computer system.

(vi) Indecent exposure

(vii) Email spoofing

(viii) Cheating & Fraud

Against Individual Property:

(i) Computer vandalism

(ii) Transmitting virus

(iii) Unauthorized control/access over computer system

(iv) Intellectual Property crimes

(v) Internet time thefts

Against Organization:

(i) Unauthorized control/access over computer system

(ii) Possession of unauthorized information.

(iii) Cyber terrorism against the government organization.

(iv) Distribution of pirated software etc.

Against Society at large:

(i) Pornography (basically child pornography).

(ii) Polluting the youth through indecent exposure.

(iii) Trafficking

(iv) Financial crimes

(v) Sale of illegal articles

(vi) Online gambling

(vii) Forgery

1.19 Information Technology Act

The Information Technology Act deals with the following cybercrimes along with others.

Tampering with Computer Source Documents

A person who knowingly or intentionally, conceals (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable.

For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file. Hacking is usually understood to be the unauthorized access of a computer system and networks. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code Hacker, Cracker or a Cyber Punk.

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 means is said to commit hacking.

Publishing Obscene Material in Electronic Form

A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produce the effect of publishing), pornographic material in the electronic form. Child Pornography Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cybercrime. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cybercrime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start contacting children on their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object. Accessing protected system Any unauthorized person who secures access or attempts to secure access to a protected system is liable to be punished with imprisonment and may also be liable to fine.

Breach of Confidentiality and Privacy

Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document

or other material to any other person shall be liable to be punished under the Information Technology Act.

Notes

1.20 Relevant Cyber Crimes other than IT Act, 2000

Cybercrimes other than those mentioned under the IT Act

Cyber Stalking

Although there is no universally accepted definition of cyber stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using Internet services. Stalking in general terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

Cyber Squatting

Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different).

A trademark owner can prevail in a cyber squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of -pocket expenses.

Data Diddling

This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed.

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

Cyber Defamation

Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Trojan Attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners. It is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in college.

Financial Crimes

This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

Internet Time Theft

This con notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cybercrime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

Virus/Worms Attack

Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

E-mail Spoofing

It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about

him by spoofing B's email address, this could result in ending of relations between B and his friends.

Email Bombing

Notes

Email bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider.

Salami Attack

This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alteration is so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a programme whereby a meager sum of ₹ 3 is deducted from customers account. Such a small amount will not be noticeable at all.

Web Jacking

This term has been taken from the word hijacking. Once a website is web jacked the owner of the site loses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site. Rehabilitation

1.21 Misuse of Technology in the form of Cyber Crime

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer- related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighboring rights. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data.

1.22 Cyber Crime in Modern Society

Today, criminals that indulge in cybercrimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cybercrimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cybercrimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need

not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

Notes

1.23 Categories of Cyber Crime

Cybercrimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual: This type of cybercrime can be in the form of cyber stalking, distributing pornography, trafficking and grooming'. Today, law enforcement agencies are taking this category of cybercrime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

1.24 Different Kinds of Cyber Crime

The different kinds of cybercrimes are:

1. **Unauthorized Access and Hacking:** Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready- made computer programs to attack the target computer. They possess the desire to destruct and they

Notes

get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

A hacker is an unauthorized user who attempts to or gains access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an invasion in to the privacy of data. There are different classes of Hackers.

(a) ***White Hat Hackers:***They believes that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hat hackers who are just joy riding" on computer systems.

(b) ***Black Hat Hackers:*** They cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also called—crackers.

(c) ***Grey Hat Hackers:*** Typically ethical but occasionally violates hacker ethics Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting malware (viruses or worms).

2. **Web Hijacking:** Web hijacking means taking forceful control of website of others. In this case the owner of the website loses control over his website and its content.
3. **Pornography:** Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.
4. **Child Pornography:** The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cybercrime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them

some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

How do they operate?

(a) Pedophiles use false identity to trap the children/teenagers.

(b) Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.

(c) Befriend the child/teen.

(d) Extract personal information from the child/teen by winning his confidence.

(e) Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address?

(f) Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him are normal and that everybody does it.

(g) Extract personal information from child/teen.

(h) At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

5. **Cyber Stalking:** In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber stalking means repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services. Both kinds of stalkers i.e., Online & Offline have desire to control the victims life.

How do Cyber Stalkers operate?

(a) They collect all personal information about the victim such as name, family background, telephone numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

Notes

(b) The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

(c) People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

(d) Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

(e) Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

(f) In online stalking the stalker can make third party to harass the victim.

(g) Follow their victim from board to board. They hangout on the same as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will flame their victim (becoming argumentative, insulting) to get their attention.

(h) Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

(i) Contact victim via telephone. If the stalker is able to access the victim telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

(j) Track the victim to his/her home.

6. **Denial of service Attack:** This is an attack in which the criminal floods the bandwidth of the victim network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

7. **Virus Attacks:** Viruses are the programs that have the capability to infect other programs and make copies of it and spread into other program. Programs that

multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attaches them to other software. Virus, worms, Trojan horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of them and do this repeatedly till they eat up all the available. Trojan horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

8. **Software Piracy:** Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

   Domain names are also trademarks and protected by ICANN domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider name so as to attract their users and get benefit from them.

9. **Salami Attacks:** These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank servers, that deducts a small amount of money (say ₹ 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

10. **Phishing:** Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

11. **Sale of illegal articles:** This category of cybercrimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

Notes

12. **Online gambling:** There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.
13. **Email spoofing :** E-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e- mail originated from a different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender.

    Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.
14. **Cyber Defamation"** When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person friends, it is termed as cyber defamation.
15. **Forgery:** Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.
16. **Theft of information contained in electronic form:** This includes theft of information stored in computer hard disks, removable storage media etc.
17. **Email bombing:** Email bombing refers to sending a large number of emails to the victim resulting in the victims email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
18. **Internet time theft:** Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.
19. **Theft of computer system:** This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.
20. **Physically damaging a computer system:** This crime is committed by physically damaging a computer or its peripherals.

21. **Breach of Privacy and Confidentiality:** Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information. Confidentiality means non-disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

    Generally for protecting secrecy of such information, parties while sharing information forms an agreement about the procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

22. **Data diddling:** Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatic changing the financial information for some time before processing and then restoring original information.

23. **E-commerce/ Investment Frauds:** An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

24. **Cyber Terrorism:** Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

    Cyber terrorism is an attractive option for modern terrorists for several reasons.

    - It is cheaper than traditional terrorist methods.
    - Cyber terrorism is more anonymous than traditional terrorist methods.

Notes

- The variety and number of targets are enormous.
- Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
- Cyber terrorism has the potential to affect directly a larger number of people.

1.25 How to Tackle Cyber Crime

It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.

The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe

1.26 Major Threats of Cyber Crime in the Current Scenario

Well at present, cases such as credit card thefts and online money-laundering are on the rise. Cybercrime has also exposed the impending hazards of e-banking. Zenophobia, hate-mail cases and cyber-terrorism are the most pronounced aspects of cybercrime across countries. Fake escrow scams, online infringement of music, videos and software also having big impact in cybercrime. Well, as far as India is concerned, I don't see very effective laws in place to address such cases. However, I appreciate the amendment made in the IT Act, 2000. When the IT Act was passed way back in 2000, the Act majorly addressed issues related to e-commerce.

1.27 Impact of Cyber Crime on Businesses

As all the businesses, all over the world are increasingly operating in the online mode because most of their work being done through websites, hence all sectors are equally vulnerable to cybercrime. Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. However, I would say that SMEs in the IT industry are the greatest stake holders. Piracy and copy right protection are the major threats.

1.28 Cyber Laws

Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1. Cybercrimes under the IT Act
   - Tampering with Computer source documents - Sec.65
   - Hacking with Computer systems, Data alteration - Sec.66
   - Publishing obscene information - Sec.67
   - Un-authorized access to protected system Sec.70 Breach of Confidentiality and Privacy - Sec.72
   - Publishing false digital signature certificates - Sec.73
2. Cyber Crimes under IPC and Special Laws
   - Sending threatening messages by email - Sec 503 IPC
   - Sending defamatory messages by email - Sec 499 IPC
   - Forgery of electronic records - Sec 463 IPC
   - Bogus websites, cyber frauds - Sec 420 IPC
   - Email spoofing - Sec 463 IPC
   - Web-Jacking - Sec. 383 IPC
   - E-Mail Abuse - Sec.500 IPC
3. Cyber Crimes under the Special Acts
   - Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
   - Online sale of Arms Act

1.29 Prevention of Cyber Crime

Notes

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.
- One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cybercrimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the legislatures keeping in mind the interest of netizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

- A complete justice must be provided to the victims of cybercrimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cybercrime.

Notes

1.30 Misuse of technology

Cyber-criminals should be aware that no matter where in the world you commit cybercrime, even from remote places, you can and will be identified and held accountable for your actions.

1.31 Computer Forensics Defined

Judd Robbins', an explanation of Computer Forensics, definition of computer forensics is as follows: Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud.

Jerry Wegman, an Associate Professor of Business Law, states, Computer forensics has developed as an indispensable tool for law enforcement. But in the digital world, as in the physical l world, the goals of law enforcement are balanced with the goals of maintaining personal liberty and privacy. Computer forensic investigators must be aware of the legal environment in which they work, or they risk having the evidence they obtain being ruled inadmissible.

Ms. Erin Kenneally further defines computer forensics by stating, Since forensic science is the application of a scientific discipline to the law, the essence of all forensic disciplines concerns the principles applied to the detection, collection, preservation, and analysis of evidence to ensure its admissibility in legal proceedings. Computer forensics refers to the tools and techniques to recover, preserve, and examine data stored or transmitted in binary form.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Notes

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

1.32 Objectives of Cyber Forensics

The objective of Cyber forensics is to identify digital evidence for an investigation with the scientific method to draw conclusions. Examples of investigations that use cyber forensics include unlawful use of computers, child pornography, and cyber terrorism.

The area of cyber forensics has become prominent field of research because:

1. Forensics systems allow the administrator to diagnose errors
2. Intrusion detection systems are necessary in avoiding cyber crimes
3. Change detection can be possible with proactive forensics

Cyber forensics can be used for two benefits:

- To investigate allegations of digital malfeasance
- To perform cause analysis

1.33 Legal Scenario

Forensic evidence is only as valuable as the integrity of the method that the evidence was obtained. The methods applied to obtain evidence are best represented if standards are known and readily established by the digital forensics community. The Fourth Amendment limits the ability of government agents to perform search and seizure evidence tactics without a warrant, including computers.

The Fourth Amendment states: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment question that typically comes up in digital evidence cases asks whether an individual has a reasonable expectation of privacy having electronic information stored on electronic devices under that individual's control.

Computer evidence can present a challenge for both prosecutors and defendants alike. A guide to offering mobile device data as evidence is beyond the scope of this research but a few examples of some digital forensics issues in real life situations are described below.

A legal issue in presenting evidence is the best evidence rule' which states that to prove the contents of a document, recording or photograph, the original' document, recording or photograph is ordinarily required. For example, in United States v. Bennett, 363 F.3d 947, 953 (9th Cir. 2004), a federal agent testified about information that he viewed on the screen of a GPS on the defendant's boat in order to prove he had imported drugs across international waters. It was decided the agent's testimony violated the best evidence rule because he had only observed a graphical representation of data from the GPS instead of actually observing the professed path the boat had been following during the encounter. Since the U.S. sought to prove the contents of the GPS, the best evidence rule was invoked and required the government to present the actual GPS data or printout of the data, rather than the testimony from the federal agent.

In 2010, a Japanese sumo wrestling match-fixing scandal was brought to light after investigators analyzed data left on fifty cell phones seized from wrestlers of the Japan Sumo Association (JSA) while probing a baseball scandal in that country. The Japanese police were able to retrieve and restore electronic mail messages previously deleted from the mobile phones including messages exchanged among wrestlers who were being implicated in the wrestling bout-rigging case. The sumo wrestlers refused to turn over their mobile devices to law enforcement claiming their phones were damaged due to water or the battery had died in the phones. The case is still ongoing in Japan but members of the JSA plan to obtain data left on the cell phones utilized by the suspected wrestlers to restore deleted email messages in order to prove the case against the sumo wrestlers. Even if deleted, the cell phone email data remains in binary format on the handheld device's memory. This is called data remanence or the residual representation of data that remains after attempts have been made to remove or erase the data. Through digital forensics, even mobile devices that have been ruined or immersed in water can still recover data unless the device's memory chips are destroyed.

Like digital evidence from a computer, it is necessary to have proper legal authority in order to perform a forensics investigation of cellular telephones and mobile handheld devices. An exception that is supported by case law (U.S. v. Finley C.A.5 Tex., 2007, & U.S. v. Carroll N.D. Ga. , 2008) allows a search incident to arrest' and is often connected with searches of arrestees and motor vehicles. For example, in the U.S v. Finley case, it was noted that the defendant in the case had conceded that a cell phone was analogous to a closed container' for the purpose of Fourth Amendment analysis. Such searches are allowed by the court to be performed for the preservation of evidence that could easily be altered or damaged. This exception for handheld devices is restricted by a limited period of time and according to law, may be searched without a warrant only if the search is substantially contemporaneous with the arrest (U.S. v. Curry D Me., 2008). The authors

Notes

of the Fourth Amendment could not have envisioned the powerful technology of today's electronic age and courts have only begun to answer difficult questions that are being introduced through the use of these devices. Current Fourth Amendment doctrine and precedent cases suggest that the United States Supreme Court would consent to invasive searches of a mobile device found on the person of many individuals and has allowed an exception permitting warrantless searches on the grounds that law enforcement should be allowed to look for weapons or other evidence that could be linked to an alleged crime. The Obama administration and many local prosecutors feel that warrantless searches are perfectly constitutional during arrests.

Privacy advocates feel that existing legal rules allowing law enforcement to search suspects at the time of an arrest should not apply to mobile devices like the smart phone because the value of information being stored is greater and the threat of an intrusive search is much higher, such as PII. Personally identifiable information (PII) is information connected to an individual including but not limited to education, financial transactions, medical information, and criminal or employment history which can be used to trace that individual's identity such as name, social security number, or birth date. While technologies have evolved over the years, the search incident principle has remained constant.

The Fourth Amendment applies to mobile electronic devices and digital evidence just as it does any other type of criminal evidence. Legally, when handling computers and mobile devices, it is best for the forensics investigator to treat them as they would a closed container, such as a briefcase or a file cabinet. Generally, the Fourth Amendment prohibits law enforcement personnel from accessing, viewing, or examining information stored on a computer or mobile device if the law enforcer would be prohibited from opening a closed container and examining its contents in the same situation. The forensics investigator should always be aware that laws vary state by state and unopened electronic mail, unread texts, and incoming phone calls of seized devices may present non-consensual eavesdropping issues.

In digital media searches, the media is frequently searched off site and in an enclosed forensics laboratory. Generally, courts have treated the offsite forensics analysis of seized digital media as a continuation of the initial search and thus, the investigator is still bound by the Fourth Amendment. Because this analysis is often treated as part of the initial search, the government bears not only the burden of proving the seizure was reasonable and proper, but also that the search was conducted in a reasonable manner. To ensure that search and seizure forensics analysis meets the burden later at the trial, the forensics investigator should generate a written report with clear documentation of the analysis.

Notes

1.34 Legal Provisions in Indian Perspective

The confluence of two legal paradigms, i.e., the law of evidence and that of information technology has made the legal domain at par with the contemporary challenges of the cyber space.

1. Firstly, the traditional law defining the term Evidence' has been amended to include electronic evidence in Section 3, The Evidence Act, 1872. The other parallel legal recognition appeared in Section 4, The Information Technology (Amendment) Act, 2008, with the provision for acceptance of matter in electronic form to be treated as written' if the need arises. These show a prima faci acceptability of digital evidence in any trial.
2. Further, Section 79A of the IT (Amendment) Act, 2008 has gone aboard to define electronic evidence as any information of probative value that is either stored, or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines.
3. With regards to admissibility of electronic records, Section 65-B of the Evidence Act, 1872 enunciates various conditions for the same.
4. Since digital evidence ought to be collected and preserved in certain form, the admissibility of storage devices imbibing the media content from the crime scene is also an important factor to consider. Reading Section 3 and Section 65-B, The Evidence Act, 1872 cumulatively, it can be inferred that certain computer outputs of the original electronic record, are now made admissible as evidence without proof or production of the original record. Thus, the matter on computer printouts and floppy disks and CDs become admissible as evidence.
5. The other most crucial question in cybercrime investigation regarding the reliability of digital evidence has also been clarified by Section 79A of the IT (Amendment) Act, 2008, which empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence. This agency will play a crucial role in providing expert opinion on electronic form of evidence.

1.35 Phases of Cyber Forensics

Identification Phase

The identification phase is the process of identifying evidence material and its probable location. This phase is unlike a traditional crime scene it processes the incident scene and documents every step of the way. Evidence should be handled properly. Basic requirement in evidence collection is evidence must be presented without alteration. This

Notes

requirement applies to all phases of forensics analysis. At the time of evidence collection, there is a need of thorough check of system logs, time stamps and security monitors.

Once evidence collected, it is necessary to account for its whereabouts. Investigators would need detailed forensics to establish a chain of custody, the documentation of the possession of evidence. Chain of custody is a vital part of computer forensics and the legal system and the goal is to protect the integrity of evidence, so evidence should be physically secured in a safe place along with a detailed log.

The evidence and chain of custody which is useful during incident investigation. Handling specific type of incidents like Denial of Service, Malicious Code, Unauthorized access etc. are described in computer security incident handling guide.

Acquisition Phase

The acquisition phase saves the state of evidence that can be further analyzed. The goal of this phase is to save all digital values. Here, a copy of hard disk is created, which is commonly called as an image. Different methods of acquiring data and their relative advantages and disadvantages are described in. As per law enforcement community, there are three types of commonly accepted forensics acquisition: mirror image, forensics duplication and live acquisition.

Mirror images, bit-for-bit copy, involve the backups of entire hard disk. Creation of mirror image is simple in theory, but its accuracy must meet evidence standards. The purpose of having mirror image is evidence available in the case of the original system need to be restarted for further analysis. Data and their relative advantages and disadvantages are described in as per law enforcement community; there are three types of commonly accepted forensics acquisition: mirror image, forensics duplication and live acquisition.

Mirror images, bit-for-bit copy, involve the backups of entire hard disk. Creation of mirror image is simple in theory, but its accuracy must meet evidence standards. The purpose of having mirror image is evidence available in the case of the original system need to be restarted for further analysis.

Analysis Phase

Forensic analysis is the process of understanding, recreating and analyzing arbitrary events that have gathered from digital sources. The analysis phase collects the acquired data and examines it to find the pieces of evidences.

This phase also identify that the system was tampered or not to avoid identification. Analysis phase examines all the evidence collected during collection and acquisition phases. There are three types of examinations can be applied for the forensics analysis; limited, partial or full examination.

Reporting Phase

The reporting phase comprises of documentation and evidence retention. The scientific method used in this phase is to draw conclusions based on the gathered evidence. This phase is mainly based on the Cyber laws and presents the conclusions for corresponding evidence from the investigation. There is a need of good policy for how long evidence from an incident should be retention. Factors to be considered in this process are prosecution, data retention and cost. To meet the retention requirements there is a need of maintaining log archival. The archived logs must be protected to maintain confidentiality and integrity of logs.

1.36 Forensics Methodology

The International Association of Computer Investigative Specialists (IACIS) has developed a forensic methodology which can be summarized as follows:

- Protect the Crime Scene, power shutdown for the computer and document the hardware configuration and transport the computer system to a secure location
- Bit Stream backup of digital media, use hash algorithms to authenticate data on all storage devices and document the system date and time
- Search keywords and check file space management (swap file, file slack evaluation, unallocated space)
- Evaluate program functionality, document findings/results and retain Copies of software.

1.37 Cyber Forensic Tools

The main objective of cyber forensics tools is to extract digital evidence which can be admissible in court of law. Electronic evidence (e-evidence, for short) is playing a vital role in cybercrimes. Computer forensics tools used to find skeletons in digital media. To reduce the effect of anti-forensics tools the Investigator is likely to have the tools and knowledge required to counter the use of anti-forensics techniques.

1. The Coroner's Toolkit (TCT), is an open source set of forensic tools designed to conduct investigation UNIX systems.
2. Encase is the industry standard software used by law enforcement
3. The Forensic Toolkit (FTK) is very powerful tool but not simple to use.
4. 12Analyst is a different type of analysis tool; it is visual investigative analysis software.
5. LogLogic's LX 2000 is powerful and distributed log analysis tool.

Notes

6. Net Witness and security intelligence are network traffic security analyzer tools.
7. ProDiscover Incident Response (IR) is a complete IT forensic tool that can access computers over the network to study the network behavior
8. The Sleuth Kit is one of network forensics tools used to find file instances in an NTFS file.

1.38 Case Laws

State of Maharashtra vs. Dr. Praful B Desai (AIR 2003 SC 2053)

[The question involved whether a witness can be examined by means of a video conference.]

The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing, and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.

Rajesh and Nupur Talwar Would File Appeal At Allahabad High Court Today

The Aarushi Talwar's murder case is a real complicated one. There is no direct evidence and the case has been decided based upon circumstantial evidences. A CBI judge, in November 2013, held that the parents of Aarushi Talwar are guilty of the murder of their daughter and domestic help.

Now the convicted couple has decided to file an appeal before the Allahabad High Court on Tuesday i.e. 21-01-2014. An application for bail had also been attached with the appeal, with the matter likely to be listed for Thursday. The appeal runs into 2,200 pages, with the grounds for appeal being 600 pages long.

The lawyers for the convicted accused parents are appealing against issues like nature of burden of proof, improper witnesses and evidence, etc. These seem to be traditional criminal law related arguments.

The lawyers of the convicted parents seem to have ignored the digital evidence that, if proved successfully, could easily lead to their acquittal. This is more so when the central bureau of investigation (CBI) has failed to produce very credible cyber forensics evidence In the lower court.

When stakes are high it is not a good strategy to ignore and exclude crucial areas that can strengthen a lawyer's case. Let us see how the appeal would be pursued at the Allahabad High Court in the near future.

Jagjit Singh vs. State of Haryana ((2006) 11 SCC 1)

The speaker of the Legislative Assembly of the State of Haryana disqualified a member for defection. When hearing the matter, the Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel, the AajTak television channel, and the Haryana News of Punjab Today television channel.

The court determined that the electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action. The Supreme Court found no infirmity in the speaker's reliance on the digital evidence and the conclusions reached by him. The comments in this case indicate a trend emerging in Indian courts: judges are beginning to recognize and appreciate the importance of digital evidence in legal proceedings.

1.39 Misuse of computer forensics

Computer forensic evidence often plays a key role in serious crime investigations, helping to track and analyze criminal behavior through data stored on privately owned computers and mobile devices. There is, however, a growing trend of computer misuse in the workplace, and more public and private sector organisations now look to the experts to uncover this evidence discreetly and without disrupting business continuity.

1.40 Indian Evidence Act, 1872

The Indian Evidence Act, 1872 contains set of rules and regulations regarding admissibility of evidence in the Indian Courts of law. Indian Evidence Act was passed by the British Parliament in 1872 setting up a path-breaking judicial measure by changing traditional legal systems of different social groups and communities. Since then from time to time amendments are made in the Indian Evidence Act to make it compatible with changing times.

The Information Technology Act was originally passed on 17th October 2000 with one of the aim to provide legal recognition to digital/electronic evidence. Hence, amendments were made in the Indian Evidence Act regarding collection and production of digital evidence in the court of law.

Some of the important provisions of the Indian Evidence Act pertaining to digital/ electronic evidence are as follows:

- Sec. 2(1) (t) Defining Electronic Record

"Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

The section has made electronic record legally admissible in the court of law.

- Sec. 3 (a) – Scope of definition of evidence expanded to include electronic records.

Notes

- Sec. 65B – Admissibility of electronic records

The person owning or in-charge of the computer from which the evidence is taken has to give certificate as to the genuineness of electronic record.

- Sec. 88A – Presumption as to electronic messages

The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

1.41 Provisions of Indian Evidence Act, 1872 followed with Information Technology Act, 2000

Section 65A: Special provisions as to evidence relating to electronic record. The contents of electronic records may be proved in accordance with the provisions of section 65B".

Section 65B- 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 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:
   (i) 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;
   (ii) 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;

(iii) 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

(iv) 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.

(v) 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 (b) was regularly performed by computers, whether-

(i) by a combination of computers operating over that period; or

(ii) by different computers operating in succession over that period; or

(iii) by different combinations of computers operating in succession over that period; or

3. 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,

(i) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(ii) 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;

(iii) Dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the 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:

(i) 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;

Notes

(ii) 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;

(iii) 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 there from by calculation, comparison or any other process.

After section 67, the following section shall be inserted, namely: Proof as to digital signature. "67A. except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved."

After section 73, the following section shall be inserted, namely: - Proof as to verification of digital signature. '73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct- (a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate; (b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person. Explanation-For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000.

After section 81, the following section shall be inserted, namely: - 81 A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.

After section 85, the following sections shall be inserted, namely: 85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties. Section 85B refers as presumption of electronic records and digital signatures. 85B. (1) 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.(2) In any proceedings, involving

secure digital signature, the Court shall presume unless the contrary is proved that- (a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record; (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Presumption as to Digital Signature Certificates

Presumption as to Digital Signature Certificates.-The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

After section 88, the following section shall be inserted, namely: 88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent. Explanation--For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.

After section 90, the following section shall be inserted, namely: 90A. Presumption as to electronic records five years old.- Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable. This Explanation applies also to section 81A.

For section 131, the following section shall be substituted, namely: Production of documents or electronic records which another person, having possession, could refuse to produce. "131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

1.42 Digital Evidence – Technological & Practical Issues

Notes

Types of Digital Evidence

Data in desktops, laptops, tablets & cell phones, Data on pendrives, CD, DVD, Encrypted data, Steganographic data, Password protected data, GPS data in photographs, Data on the cloud, Network data, Databases.

Extraction and Production in court of Digital Evidence

Email evidence, Facebook evidence, Photographs (from smartphones, digital cameras), Text, whatsapp and iMessage evidence, Evidence in browsers, Digital signatures as evidence, Deleted data, IP addresses, Wi-Fi and server logs.

Digital Evidence & the Indian Law

- Relevant provisions of the Indian Evidence Act, 1872 as amended by the Information Technology Act – sections 3, 17, 22A, 34, 35, 39, 47A, 59, 65A, 65B, 67A, 73A, 81, 85A, 85B, 88A, 90A, 131
- Relevant provisions of the Bankers' Books Evidence Act, 1891 as amended by the Information Technology Act - sections 2, 2A
- Relevant provisions of the Information Technology Act – section 79A - Examiner of Electronic Evidence
- Case Law - Amitabh Bagchivs EnaBagchi, 2004 Ark Shipping Co. Ltd. Vs Grt Ship management Pvt. Ltd., Bodala Murali Krishna vs Smt. Bodala Prathima, Dharambirvs Central Bureau Of Investigation, Jagjit Singh vs State Of Haryana &Ors, KN Govind acharya v Union of India & others, State vs Mohd. Afzal and Ors. State Bank of India vs Rizvi Exports Ltd., State (N.C.T. Of Delhi) vs Navjot Sandhu @ Afsan Guru, Twentieth Century Fox Film vs Nri Film Production Associates
- Case Law (Adjudicating Oficers & CCA) - Arhan Technologies Pvt. Ltd, Thomas Raju v ICICI Bank, Sourabh Jain v ICICI Bank and Idea Cellular Ltd., Rohit Maheshwari v Vodafone & others, Sanjay Govind Dhande & others v ICICI

Bank & others, Umashankar Sivasubramanian v ICICI Bank & others, CCA order in the matter of Yahoo India.

1.43 Cyber Crimes – Law, Investigation & Adjudication

1. **Offences under the Information Technology Act:** Computer related offences (section 43 and 66), Computer source code related offences (section 43 and 65),

Failure to protect data (section 43A), Sending offensive messages (section 66A), Dishonestly receiving stolen computer (section 66B), Identity Theft (section 66C), Cheating by personation (section 66D), Violation of privacy (section 66E), Cyber Terrorism (section 66F), Transmitting obscene electronic material (section 67), Electronic material containing sexually explicit act (section 67A), Child Pornography (section 67B), Preservation and retention of information by intermediaries (section 67C), Power of the Controller to give directions. (section 68), Interception or monitoring or decryption of any information (section 69), Blocking of information for public access (section 69A), Monitoring and collecting traffic data (section 69B), Protected System (section 70), Indian Computer Emergency Response Team (section 70B), Penalty for misrepresentation (section 71), Breach of confidentiality and privacy (section 72), Disclosure of information in breach of lawful contract (section 72A), Publishing false Electronic Signature Certificate (section 73), Publication for fraudulent purpose (section 74).

2. **Investigation issues:** Power to investigate offence (section 28, 78), Power of police officer (section 80).
3. **Related issues:** Extradition Issues (section 75), Confiscation (section 76), Compounding of offences (section 77A), Bailable & cognizable offences (sections 77A, 77B), Liability of intermediary (section 79), Abetment (section 84B), Offences by companies (section 85), Blocking of websites.
4. **Adjudication issues:** 45, 46, 47, Chapter 10 and Information Technology (Qualification and experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003.
5. **Documentation Issues:** First Information Report, Property Search & Seizure Form, Final Form/ Report, Relevant checklists, relevant reports. Rehabilitation

1.44 Misuse of technology

Any data which is transferred online is subject to the risk of being intercepted and misused. Encrypting data before transferring it over the internet will go a long way in safeguarding against such interception. Even though the data may be intercepted it would be of no use unless it is decrypted. If encryption of data is adopted by all entities providing services through the internet then it would extremely helpful in protecting the customers privacy and also in protection of all other data. At present, the data encryption standards imposed on different categories of online service providers are not uniform.

1.45 Computer Forensics

Computer forensics can be categorized in two categories: firstly, the discovery, recovery, preservation and control of electronic data has been investigate, secondly, the analysis,

Notes

verification and presentation of e-evidence has been done and present in court of law for further proceedings. The collection of electronic evidence must be followed with five basic rules as follows:

- First one is admissibility which is the most basic rule to be followed in court of law.
- Evidence should be authentic, if it should not tie with the incident positively, then it should be difficult to prove anything with the use of that evidence.
- It should be complete and reliable. Since, an evidence collection and analysis procedures must not cast doubt on the authenticity of the evidences.
- Lastly, the evidence which is presented in front of jury should be understandable and believable.

While, if it should be followed with general procedure of collecting and analyzing evidence. Then there are four step procedures which an official have to be followed during the time of investigation i.e. identification of evidence, preservation of evidence, analysis of evidence and finally presentation of evidence. However, if we deal with the collection procedure of digital or electronic evidence then in this situation an official follows such steps i.e.

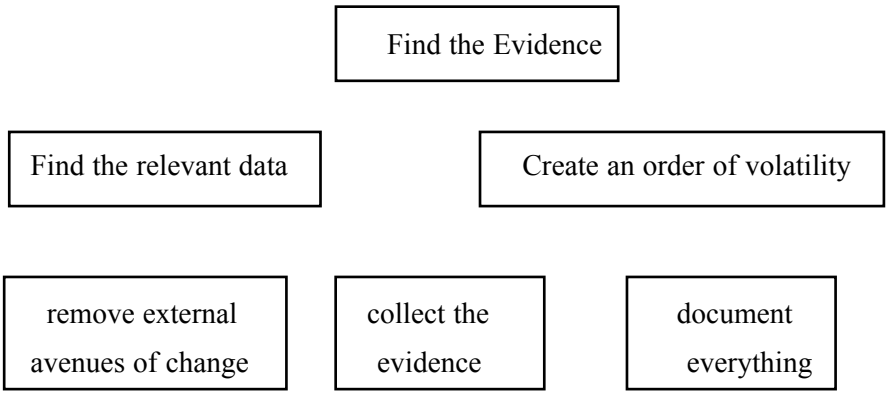


Fig. Collection Steps

Although, the major step followed for controlling the contamination of evidences is the chain of custody where the data once collected, then it should get protected from contamination. Because during forensic examination originals should not be used only verified duplicates should be used. A good way of ensuring the data to be uncorrupted is to keep a Chain of Custody which is a detailed list of what was done with the original copies once they were collected. The chain of custody follows step by step procedure in which officials are categorized in different categories.

Digital evidence is consider as all the digital or electronic sources which can be gather during investigation and contains any type of information in it which may be

used as evidence in that particular case. Meanwhile, it is a part of computer forensics where some special techniques have been use for preserving, identification, analysis, examination, authentication, interpretation and documentation of digital information. Computer forensics is a mandatory process in the field of investigation where digital evidence should be gathered and processed in the court of law. However, the preservation of digital evidence must be fall under some categories, as it depends on the type and place of crime. Like if crime happens in any business organization/firm then some other steps have been followed by investigation team for preserving of digital evidence, while if it happens in any other destination then different steps should be following. Else in the process of preservation of digital evidences different types of risks may occur and to combating them an investigation team should be prepared with mitigation practices. Let us discuss the following categories with *preservation steps:*

1. Stand-alone home computer
   - Don't try an attempt to use computer.
   - Photograph it from front and back side.
   - Unplug all power cords.
   - Seize additional storage media.
   - Collect instruction manuals, documents and notes.
   - Prepare the documentation of all steps involved in the seizure of a computer.
2. Home Networked system
   - Unplug power to router or modem.
   - Rest of the procedure is same as above.
3. Business Network
   - A computer specialist should be consulted in case of preserving business servers.
   - A team has to secure the scene and prevent handling of any networking devices except professional.
   - Because in these matters in anyone pull out the plug then it may cause damage to the system or loss of data.
4. Storage Media
   - Used to store data from electronic devices.
   - Keep away from magnets, radio transmitters and other potentially damaging devices.

5. Personal Digital Assistances

- If the device is —'on', leave it on because if it is powered down then the device could enable password.
- Keep device charged.
- Seize additional storage media.

Notes

(FILL IN ONE FORM PER ITEM SEIZED)

FIRST RESPONDER SEIZURE RECORD

Case No.		Case Name	

Location of Seizure

Full Address	Room No Building Address Line 1 Address Line 2 Address Line 3 Address Line 4 Post Code	

Details of Evidence Seized

Type (E.g. computer, disk, paper etc)		Where Located	
Make		Model	
Serial No.		Evidence bag no.	

Acquisition Details

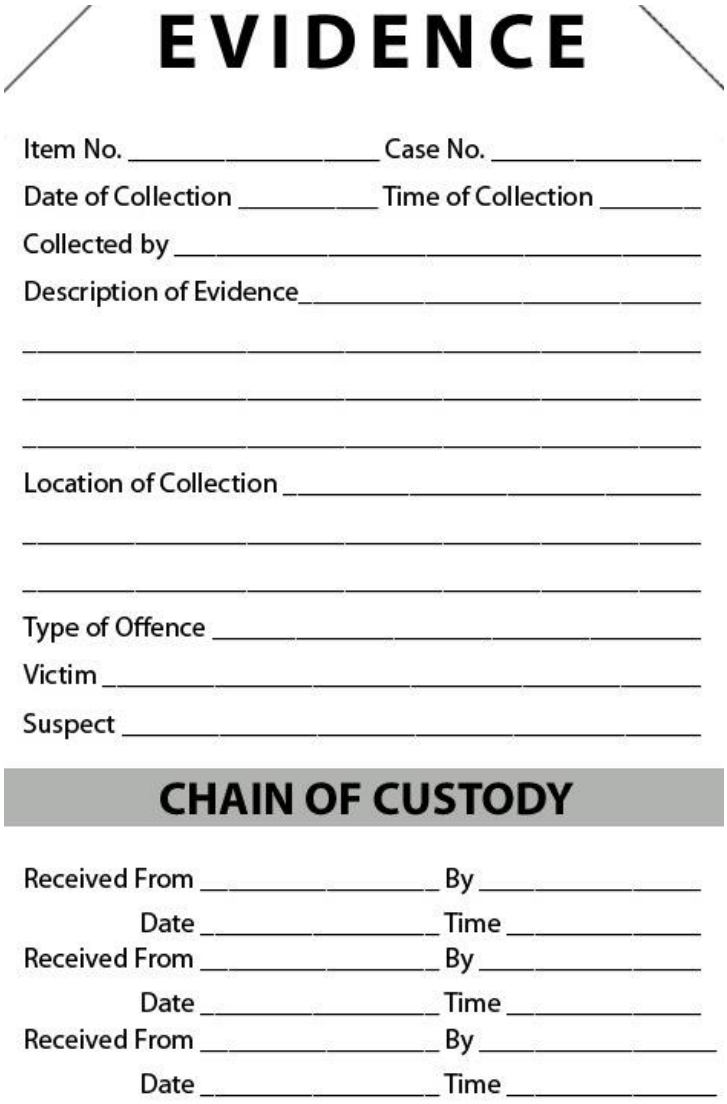
Have you enquired of the owner any password used ?	YES	NO
If yes to above please state password and how used.		
Was the equipment attached to a telephone line at time of the seizure ?	YES	NO
Was the equipment switched on at the time of seizure ?	YES	NO
If yes to above please state how equipment was switched off and secured.		
Has the equipment been switched on since being seized ?	YES	NO
If yes to above please state the reason and the details of the person.		

Photo of exhibit taken (if so attach them)	YES	NO	Sketch produced (if so attach it)	YES	NO

Witness Signature (Forensic Analyst making seizure)			
Full Name		Title	
Phone		Department	

Fig. 1.1: Seizure Form

Notes



EVIDENCE

Item No. _____ Case No. _____

Date of Collection _____ Time of Collection _____

Collected by _____

Description of Evidence_____

_____

_____

_____

Location of Collection _____

_____

_____

Type of Offence _____

Victim _____

Suspect _____

CHAIN OF CUSTODY

Received From _____ By _____

Date _____ Time _____

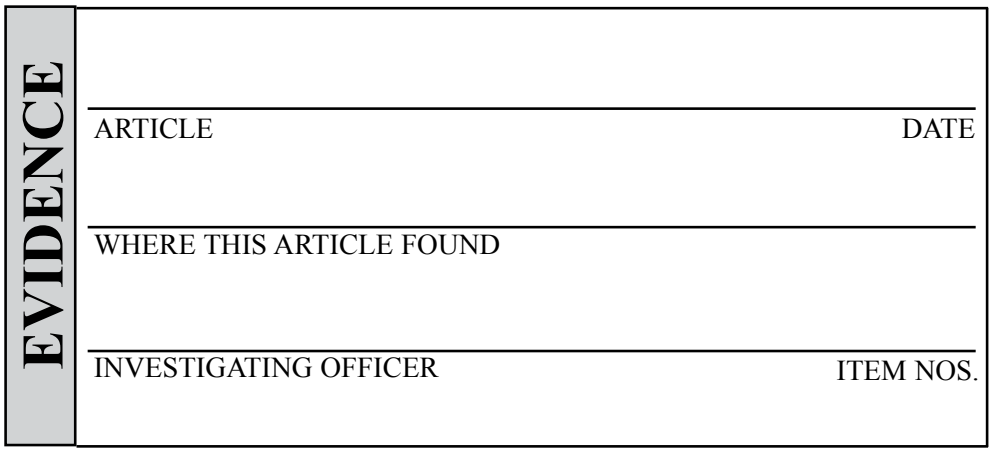
Received From _____ By _____

Date _____ Time _____

Received From _____ By _____

Date _____ Time _____

Fig. 1.2: Evidence collection and chain of custody form



EVIDENCE

ARTICLE DATE

WHERE THIS ARTICLE FOUND

INVESTIGATING OFFICER ITEM NOS.

Fig. 1.3: Sticker of Evidence

1.46 Legal Scenario

Notes

Information and communication systems are becoming popular platform in the grounds for collecting electronic-evidence in processes like investigations, audits, or litigation. Since, court can also proceed with e-evidence or ask for such evidences by the investigating authority that can perform these tasks. Such authorities acquire all e-records includes telephone logs, e-mail and instant messaging which are to be preserved carefully. Since, the content and preservation of e-records will be a subject which causes different problems in litigation and investigation exercises under some new legislation which has been opted by government of different countries for preserving digital evidences or e-records. In any investigation process of digital evidence consent of legal advisor must be necessary who guide the officials with rules and regulations. This may be done because there are many agencies who indicate themselves that they have power or legal authority for gathering of digital evidence. While, some of them use their powers, acquire search warrant or court order for seizing evidence because in many countries there is not a single explicit legal provision in their national law.

US opt various acts and rules for preservation of e-records such as Sarbanes-Oxley Act (SOX) which was signed in 2002 where data retention and preservation issues were arises, Federal Rules of Civil Procedure (1970) which deals with all types of conducts and activities, another is Federal Rules of Discovery which has been assign the duty for preserving the documents. However, if we concentrate in Indian scenario then we came to know that there are very few rules or regulations followed by Indian government in preserving digital or electronic evidences i.e. Information Technology Act, 2000 and Indian Penal Code (1860). Where not a single section deals with preservation of digital evidences but co-relates with some provisions of these acts. Although, nowadays many countries are going to opt or follow international standard of ISO/IEC 27037 which deals with information technology- security techniques- guidelines for identification, collection, acquisition, and preservation of digital evidence.

1.47 Flaws in Current Scenario

The investigation and preservation of digital evidence is much vast in itself. Although, government has been facing different problems in solving the case related to cyber world. This happens because officials didn't consist of least knowledge about technologies which are eroded day by day and replacing the old one. In current setup where cybercrime affect the nation and in this situation investigation process is facing number of problems from its officials. Because of lack of technical knowledge, didn't aware of forensics process, haven't any idea of rules and regulation and many other.

However, cyber cells are developing in each state or city for combating these cybercrimes but still the officials consists lack of knowledge. This is because the government didn't provide a chance to youngster's who have that much of skills and are qualified professionals, as they promote their staff on the basis of deputation like the constable of a police station now become a typist in cyber cell. If such things happen then it cause delay in the process of solving cybercrime. To get rid away from this an official must now about search and seizure process, chain of custody, management of documentation, and also legalities of searches. Nowadays cyber experts are increasing day by day who support police officials in investigation process.

1.48 Misuse of Cyber Forensics and Investigation

Computers present new considerations for both substantive criminal law and criminal procedure. At the heart of many of the questions is the appropriate balance between privacy rights and necessary criminal investigation. It is particularly problematic with respect to computer crimes, since serious national security issues can arise when computers are misused.

1.49 Summary

The boundaries of cybercrimes, actually, are not so clear. For example, if someone uses high-tech hacking into a computer or server, getting something valuable, it's hard to say it must be a "theft" in tool cybercrime or a "hacking" in target cybercrime. So why do we still categorize cybercrime? I think we can analyze cybercrime better and more efficiently by this way. Although there are some intersections, with categorization, we will focus on each part of cybercrime respectively and then have a comprehensive concept finally.

In following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. Since Internet was invented, people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental.

Cybercrimes have become a real threat today and are quite different from old- school crimes, such as robbing, mugging or stealing. Unlike these crimes, cybercrimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes.

Computers have become an important part of our lives and as such are involved in almost everything we do from paying bills to booking vacations. However, computer

Notes

systems have also become the mainstay of criminal activity. And when the individuals involved are brought before the courts, innocence or guilt is basically decided by testimonies and evidence. Of the two areas, evidence is probably the area most key. And when it comes to evidence' it is the accuracy of that evidence which may be the difference in determining the outcome of the trail.

India got its first codified Act in the Information Technology Act, 2000 (IT Act), which fell far short of the Industry's requirements to meet global standards. The focus if the IT Act was however recognition of electronic records and facilitation of e -commerce. Barely ten sections were incorporated in the IT Act to deal with Cyber Crime. At the time when the IT Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks, data theft, illegal access to data / accessing and removal of data without the consent of the owner, etc., were listed as civil penalties under the IT Act. The IT Industry continued to rely on self – regulation and contractual undertakings to appease its global clients, as it had done before the passing of the IT Act.

Preservation of digital evidence is a work which needs lots of effort drawn from the side of every official who are involve in investigation practice, as because the laws behind these process is much wider and complex. Since, officials didn't contain perfect knowledge of all the process; then in this situation government have to offer a workshop or session for these officials in which cyber experts share their knowledge and provide with latest tactics and standards for solving a case. And government should also show their efforts by providing country a proper regulations or rules for such process through which a confusion factor occurs less.

1.50 Review Questions

1. 'Why there is a need for cyber law? Explain in detail.
2. Discuss cyber pornography with example.
3. Explain 5 types of cybercrime that are done frequently in digital world?
4. What do you mean by cybercrime? Discuss.
5. Discuss the character of cyber criminals.
6. What do you understand by conventional and cybercrime? Explain in detail.
7. Describe some relevant crimes which are not discussed in IT Act, 2000.
8. What are the motives behind cybercrime?
9. Explain different categories of cybercrime?
10. Describe cyber stalking and cyber defamation in brief.

11. Discuss 5 kinds of cybercrime.
12. What are the major threats occur in cyber world?
13. How cybercrimes are tackling in upcoming scenario?
14. Explain the concept of cyber forensic tools with example?
15. Discuss different phases of cyber forensics.
16. What are the objectives of cyber forensics?
17. Describe the forensics methodology in digital world.
18. What are the legal regulations mentioned in cyber forensics?
19. Explain different types of digital evidences.
20. What are the practical and technological issues arises during analyzing digital evidences?
21. Discuss the process of extraction and production of digital evidences in court of law.
22. What are the primary offences discussed under IT Act, 2000?
23. How digital evidence described under Information Technology Act, 2000.
24. Discuss the steps of preserving digital evidence.
25. Describe the methods of collecting digital evidence.
26. How digital evidence is processed in court of law?
27. What is the difference between computer forensics and cyber forensics?
28. What all are the flaws of computer forensics in current scenario? Discuss.

1.51 Further Readings

- A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime
- Introduction to Indian Cyber Law by Rohas Nagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf
- Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
- Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
- Cyber Forensics in India; retrieved from http://perry4law.org/cfii/
- Digital Evidence & the Indian Law by Asian School of Cyber Laws; retrieved from http://www.asianlaws.org/del.pdf

UNIT–2

Notes

Offenses Related to Information Technology

(Structure)

Notes

2.1 Learning Objectives

After studying the chapter, students will be able to:

- Explain the criminal liability for misuse of Information Technology;
- Discuss the offences & Penalties under the Information Technology Act, 2004;
- Explain the offences under the Information Technology Act, 2004;
- Explain the civil liability under Information Technology;
- Discuss the Data Protection;
- Explain the pre censorship;
- Explain the Adjudication is done;
- Explain the Constitutional validity of section 66A of IT Act;
- About Criminalization of Online Speech and Social Media;
- Explain the Misuse of social media and freedom of speech.

2.2 Introduction

The Information Technology Act, 2000 basically deals with the legal recognition of electronic documents and that of digital signatures. This Act incorporates a separate Chapter XI entitled Offences' to deal with various cybercrimes and contraventions. This act also deals with Justice dispensation systems for various cybercrimes. The act was widely criticized on various fronts and due this criticism detailed amendments were brought in the form of IT Amendment Act, 2008. Major of such amendments were the focus on data privacy and information security. Even though legal recognition of digital signatures was already included under the original Act of 2000, but the Amendment Act, 2008 made the digital signature technology-neutral. Along with, the defining of reasonable security practices to be followed by the Corporate, the role of intermediaries was also redefined. Very importantly, the term cyber cafe' was defined under this Act. Offences like child pornography and cyber terrorism were also included is the forms of cybercrimes. Cyber terrorism has been made a heinous cybercrime under this Act and has been defined in the widest possible terms and made punishable with imprisonment which may extend to imprisonment for life and fine.

An important change that has been brought forth by the Amendment Act is that the new amendment has replaced Section 43 with Section 66. Under Section 66 the Word hacking' has been removed, but that does not mean that hacking' as an offence has been removed; instead hacking still remains an offence by the name of data theft' in this section. This section has further been widened in the form of Sections 66A to 66F.

Notes

66A deals with the sending of offensive messages through communication service, and causing annoyance to any electronic communication, and also includes the offence of misleading the recipient of the origin of such messages. Such offences can be punished with imprisonment for 3 years or fine.

66B deals with dishonestly receiving stolen computers or other communication device and such a crime can be punished with three years of imprisonment or fine of ss₹ 1 Lakh or both. 66C deals with stealing electronic signature or identity such as using another persons password or electronic signature, such an offence can be punished with three years of imprisonment or fine of ′ 1 lakh or both. Similar is the punishment under section 66D for cheating by personating through computer resource or a communication device. 66E covers the offences relating to privacy violation such as publicly publishing the information about any person's location without prior permission or consent. 66F is great importance as it deals with cyber terrorism. This Section covers a wide range of offences which can be termed as terrorism; Such as, any act denying access to any authorized person to access the computer in order to hamper the unity, integrity, security or sovereignty of the nation. Further, this section also includes the acts of access to a commuter resource without authorization. It also covers such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. All the offences that are covered under this Section can be punished with life imprisonment. Very importantly, the offences which are covered under section 66 are cognizable and non-bailable.

The major transformation from section 43 of the original act to Section 66 of the Amendment Act is that, that all the offences that were covered under Section 43 gave rise to civil liability which had its remedy in either compensation or damages. But under Section 66 of the Amendment Act if such act is done with criminal intention that is mensrea, then it will attract criminal liability having remedy in imprisonment or fine or both. Moreover, under Sections 71, 72, 73 of the Information Technology Act 2000 some acts or omissions have been made criminally liable with strict liability e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc. Section 67 of the original Act dealt with publishing or transmitting obscene material in electronic form but the scope of this section was widened by the amendment which included child pornography under section 67-B and also the act of retention of records by the intermediaries. And such offences under section 67-A will be punished with conviction of a term up to 3 years and fine of ′ 5 lakh and in case it is the second conviction then conviction will be for five years and fine of ′ 10 Lack or both. But for offence under section 67-B the provision is for stricter conviction which is for 5 years and fine of ′ 10

Lakh or both in case of first conviction, and the same will be increased to 7 years and fine of ′ 10 lakh in case of second conviction.

Notes

The ITA has sought to address and improve aspects such as technology neutrality, data protection, phishing and spam, child pornography, the liability of intermediaries and cyber terrorism. While many of these amendments are a step in the right direction, the actual drafting that implements the high level objectives suffers in many respects. For example, the previous emphasis on ―digital signatures has shifted to the technologically neutral ―electronic signatures but the changes have not been carried out thoroughly enough to expunge the old concept entirely. The current law is a bit of an abnormal document in that it contains elements of both concepts, which some attention to detail could easily have averted. Another example is that the provisions meant to combat spam and phishing end up using the dreaded ―annoyance and ―inconvenience terminology with the effect of casting the net of criminality over far more than is appropriate.

For example, mail sent with the purpose of causing ―annoyance or―inconvenience (not exactly the worst offence in the offline worl(d) could put someone behind bars.

An important set of well-intentioned but woefully inadequate provisions are those relating to the protection of data. The absence of a specific law on data protection had, in itself, garnered much criticism both within the country as well as in the context of international transactions and outsourcing. The old Act offered the feeble protection of a single provision (section 43) that dealt with unauthorized access and damage to data. In an attempt to meet industry demands and international market standards, the ITA introduced two sections that address civil and criminal sanctions. While this exercise understandably falls far short of a comprehensive law relating to data (being squeezed into an omnibus piece of technology related legislation, rather than one geared up only to deal with data), there was considerable anticipation of its role in papering over the existing cracks and provide a workable, if temporary, data protection regime.

Social media offers huge opportunities for freedom of expression. Individuals are able to see their thoughts traverse the globe in an instant; news – and its interpretation – is not automatically dependent on the filtering process of the media, or of government. The freedom of expression on Internet is a crucial challenge to address in formulating inclusive information society.

Yesterday, the Supreme Court said that no person should be arrested for posting objectionable comments on social networking sites without taking prior permission from senior police officials.

The apex court, which refused to pass an order for a blanket ban on the arrest of a person for making objectionable comments on websites, said state governments should ensure strict compliance of the Centre's January 9 advisory which said that a person should not be arrested without taking permission from senior police officials. We direct

the state governments to ensure compliance with the guidelines (issued by Centr(e) before making any arrest,' a bench of justices B S Chauhan and Dipak Misra said.

Notes

2.3 Criminal Liability for misuse of Information Technology

Criminal Liability for misuse of Information Technology under Information Technology Act, 200049 are as under:

S.No.	Section	Offence Name	Description	Penalty
1.	65	Tampering with computer source document	Intentional concealment, destruction or alteration of the computer source code which is required to be kept or maintained by law	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
2.	66	Hacking with Computer System	Destruction, deletion or alteration of any information residing in a computer resource, decreasing its value or utility or affecting it injuriously by whatever means	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
3.	67	Publishing of information which is obscene in electronic form	Publication or transmission by a person or through someone else in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such which tends 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.	On first conviction with imprisonment up to 5 years and with fine up to 1 lakh Rupees and in the event of a second or subsequent conviction with imprisonment up to 10 years and also with fine up to 2 lakh Rupees.
4.	71	Misrepresentation to the Controller or the Certifying Authority	Making any misrepresentation to, or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both

5.	72	Penalty for breach of confidentiality and privacy	Any person, who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document to any other person.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.
6.	73	Publishing Digital Signature Certificate false in certain particulars	Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that the Certifying Authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or 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.	Imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh Rupees.
7.	74	Publication for fraudulent purpose	Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.

2.4 Offences & Penalties under the Information Technology Act, 200050

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information

Notes

in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The Evidence Act, 1872, The Banker's Book's Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

2.5 Offences

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cybercrime usually includes:

1. Unauthorized access of the computers
2. Data diddling
3. Virus/worms attack
4. Theft of computer system
5. Hacking
6. Denial of attacks
7. Logic bombs
8. Trojan attacks
9. Internet time theft
10. Web jacking
11. Email bombing
12. Salami attacks
13. Physically damaging computer system

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.

Notes

3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

2.6 Offences under the IT Act 2000

5.4.1 Section 65: Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, 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 being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose 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.

Object: The object of the section is to protect the intellectual property' invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

Essential Ingredients of the Section

1. Knowingly or intentionally concealing,
2. Knowingly or intentionally destroying,
3. Knowingly or intentionally altering,
4. Knowingly or intentionally causing others to conceal,
5. Knowingly or intentionally causing another to destroy,
6. Knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programmes.

Penalties: Section 65 is tried by any magistrate.

Notes

This is cognizable and non-bailable offence.

Penalties: Imprisonment up to 3 years and / or

Fine: Two lakh rupees.

Case Laws

(i) Frios v/s State of Kerala

Facts: In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both.

It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held: The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

(ii) Syed Asifuddin Case

Facts: In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.

Held: Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

(iii) Parliament Attack Case

Facts: In this case several terrorist attacked on 13 December, 2001 Parliament

House: In this the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence should not be relied.

In Parliament case several smart device storage disks and devices, a Laptop were recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V news channels. In this case design of Ministry of Home Affairs car sticker, there was game wolf pack' with user name of ―Ashiq. There was the name in one of the fake identity cards used by the terrorist. No back up was taken therefore it was challenged in the Court.

Held: Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Notes

Section66: Hacking with the 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.

Explanation: The section tells about the hacking activity.

Essential ingredients of the section:

1. Whoever with intention or knowledge.
2. Causing wrongful loss or damage to the public or any person.
3. Destroying or altering any information residing in a computer resource.
4. Or diminishes its value or utility or.
5. Affects it injuriously by any means.

Penalties: Punishment: Imprisoned up to three years and Fine: This may extend up to two lakh rupees or with both. Case Laws:

1. R v/s Gold & Schifreen

   In this case it is observed that the accused gained access to the British telecom Prestly Gold computers networks file amount to dishonest trick and not criminal offence.

2. R v/s Whiteley.

   In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.

The perspective of the section is not merely protect the information but to protect the integrity and security of computer resources from attacks by unauthorized person seeking to enter such resource, whatever may be the intention or motive.

Cases Reported In India

Official website of Maharashtra government hacked.

The official website of the government of Maharashtra was hacked by Hackers Cool Al- Jazeera, and claimed them they were from Saudi Arabia.

Notes

Section 67: Publishing of obscene information 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 circumstance, 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.

Essential ingredients of this section:

Publishing or transmitting, or causing to be published, pornographic material in electronic form.

Penalties: Punishment:

On first conviction- imprisonment which may extend up to five years.

Fine: up to on first conviction which may extend to one lakh rupees.

On second conviction- imprisonment up to which may extend to ten years and Fine which may extend up to two lakh rupees.

Case Laws

1. The State of Tamil Nadu v/s Suhas Katti.

   Facts: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.

   Held: The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of ₹ 500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of ₹ 500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of ₹ 4000/- All sentences to run concurrently.

   The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

2. Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts: There were three accused first is the Delhi school boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public plac(e) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act 2000. In addition, the schoolboy faces a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.

Held: In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

3. DASKHINA Kannada police have solved the first case of cyber crime in the district.

A press release by Dakshina Kannada Police said here on Saturday that a Father at a Christian institution in the city had approached the Superintendent of Police with a complaint that he was getting offensive and obscene e-mails.

Police said that all the three admitted that they had done this to tarnish the image of the Father. As the three tendered an unconditional apology to the Father and gave a written undertaking that they would not repeat such act in future, the complainant withdrew his complaint. Following this, the police dropped the charges against the culprit.

The release said that sending of offensive and obscene e-mails is an offence under the Indian Information Technology Act 2000. If the charges are framed.

Section 68: Power of Controller to give Directions

- The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

Notes

- Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Explanation: Any person who fails to comply with any order under sub section (1) of the above section, shall be guilty of an offence and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The under this section is non-bailable & cognizable.

Penalties:

Punishment: imprisonment up to a term not exceeding three years

Fine: not exceeding two lakh rupees.

Section 69: Directions of Controller to a Subscriber to Extend Facilities to Decrypt Information

1. 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.
2. 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.
3. 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.

Penalties: Punishment: imprisonment for a term which may extend to seven years.

The offence is cognizable and non- bailable.

Section 70: Protected System

- The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
- The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).
- Any person who secures access or attempts to secure access to a protected system in contravention of the provision 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.

Explanation: This section grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

Penalties: Punishment: the imprisonment which may extend to ten years and fine.

Notes

Section 71: Penalty for Misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties:

Punishment: imprisonment which may extend to two years

Fine: may extend to one lakh rupees or with both.

Section 72: Penalty for Breach of Confidentiality and Privacy

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other 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.

Explanation: This section relates to any to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties:

Punishment: term which may extend to two years.

Fine: one lakh rupees or with both.

Section 73: Penalty for publishing Digital Signature Certificate

false in certain particulars

Notes

1. No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-
   - The Certifying Authority listed in the certificate has not issued it; or
   - The subscriber listed in the certificate has not accepted it; or
   - 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.
2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: The Certifying Authority listed in the certificate has not issued it or, The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties:

Punishment: imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both

Case Laws:

Bennett Coleman & Co. v/s Union of India.

In this case the publication has been stated that ―publication means dissemination and circulation. In the context of digital medium, the term publication includes and transmission of information or data in electronic form.

Section 74: Publication for fraudulent purpose

Whoever 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 extend to one lakh rupees, or with both.

Explanation: This section prescribes punishment for the following acts:

Knowingly creating a digital signature certificate for any

- Fraudulent purpose or,

- Unlawful purpose.

Knowingly publishing a digital signature certificate for any

- Fraudulent purpose or
- Unlawful purpose

Knowingly making available a digital signature certificate for any

- Fraudulent purpose or
- Unlawful purpose.

Penalties:

Punishment: imprisonment for a term up to two years. Fine: up to one lakh or both.

Section 75: Act to apply for offence or contravention

committed outside India

1. Subject to the provisions 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 the offence or contravention involves a computer, computer system or computer network located in India.

Explanation: This section has broader perspective including cybercrime, committed by cyber criminals, of any nationality, any territoriality. Case Laws:

R v/s Governor of Brixton prison and another.

Facts: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account in to the accounts of the hacker, later identified as Vladimir Levin and his accomplices. After Levin was arrested he was extradite to the United States. One of the most important issues was jurisdictional issue, the ―place of origin of the cybercrime.

Held: The Court held that the real- time nature of the communication link between Levin and Citibank computer meant that Levin's keystrokes were actually occurring on the Citibank computer.

It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by a much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.

Notes

Section 76: Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, 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.

Explanation: The aforesaid section highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

Section 77: Penalties or confiscation not to interfere with other punishments

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.

Explanation: The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

Section 78: Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Explanation: The police officer not below the rank of Deputy Superintendent of police shall investigate the offence.

Conclusion: Due to the increase in the digital technology various offences has also increased. Since new-new technology come every day, the offences has also increased therefore the IT Act 2000 need to be amended in order to include those offences which are now not included in the Act.

In India cybercrime is of not of high rate therefore we have time in order to tighten the cyber laws and include the offences which are now not included in the IT Act 2000. Rehabilitation

Notes

2.7 Misuse of technology

Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law – Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

2.8 Accrued Liability and Procedural Law

The concept of accrued liability' applies only to substantive laws' and not to procedural laws' as no one can claim a vested right' in the procedure. In India we have both substantive' and procedural' laws. The Indian Penal Code and Information Technology Act are substantive laws' whereas the Indian Evidence Act, Criminal Procedure Code and Civil procedure Code are procedural laws'. Thus, by a retrospective law the procedure can be amended, changed or even repealed. Similarly, the protection of Article 20(1) is available for and can be seeked against criminal matters only and it do not extend to civil matters'. Thus, a civil liability' can be enhanced with retrospective effect.

2.9 Data Protection

Section 43A of IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term 'sensitive personal data,' nor has it prescribed a standard and reasonable security practice'. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law. However, Explanation (ii) to Section 43A is worded in such a way that there is lack of clarity whether it would be possible for banks, (or anybody corporat(e) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two

Notes

extremes of the situation. The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs. Apart from affording protection to personal data (sensitive personal data- 43A), the IT Act, 2000 also prescribes civil and criminal liabilities (Section 43 and Section 66 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., inter alia, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record, information etc. and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of ―powers granted under IT Act, 2000.

However, the attempt is such a limited one, and so replete with shortcomings that the need for a ―proper data protection law still stands. Given the proposed initiation of the UID scheme, in particular, there is a compelling need for a robust and intelligent law in this regard. Most other countries regimes clearly do at least the following:

- Define and classify types of data (for example, in most European countries, ― personal data is any data that identifies an individual, ―sensitive personal data is data that reveals details of ethnicity, religion, health, sexuality, political opinion, etc.),
- Fine-tune the nature of protection to the categories of data (i.e., greater standards of care around sensitive personal data),
- Apply equally to data stored offline and manually as to data stored on computer systems,
- Distinguish between a data controller (i.e., one who takes decisions as to dat(a) and a data processor (i.e., one who processes data on the instructions of the data controller),
- Impose clear restrictions on the manner of data collection (for example, must be obtained fairly and lawfully),
- Give clear guidelines on the purposes for which that data can be put to and by whom (often involving a consent requirement that gives the individual a great degree of control over their data),

Notes

- Require certain standards and technical measures around the collection, storage, access to, protection, retention and destruction of data,
- Ensure that the use of data is adequate, relevant and not excessive given the purpose for which it was gathered,
- Cater for opt-in and opt-out type regimes, again to provide individuals with a measure of control over the use of their data even after the stage of initial collection (which has a huge impact on invasive telemarketing or unsolicited written communication)
- Impose a knowledge requirement and procedures for allowing individuals to seek information on what data is held on them, and
- Create safeguards and penalties that are well tailored to breaches of any of the above.

Unfortunately, and perhaps understandably, the ITA barely begins to scratch the surface of what a good data protection regime entails. The provisions that it does introduce (sections 43-A and 72-A) have glaring inadequacies. Briefly:

- The term—sensitive personal data or information is used indiscriminately without any definition,
- The provisions only cover electronic data and records, not data stored in non-electronic systems or media,
- They offer no guidance on most of the principles set out above such as in relation to accuracy, adequacy, consent, purpose, etc.,
- In the absence of the controller-processor distinction, liability is imposed on persons, who are not necessarily in a position to control data, even if it is in their possession,
- Civil liability for data breaches only arises where —negligence is involved (i.e., failure to have security procedures or failure to implement them correctly will not automatically result in damages unless negligence is proven),
- Similarly, criminal liability only applies to cases of information obtained in the context of a service contract, and requires an element of —willfulness, or a disclosure without consent or in breach of a lawful contract – this is a very limited remit aimed largely at preventing disgruntled or unscrupulous employees from dealing in company/customer data.
- In addition to the criticisms leveled at the data protection provisions, the other large subset of concerns has been in relation to the civil liberties implications of the ITA. There has been some horror expressed in various forums and media about the ITA contributing to the growth of a police state, to severe curtailment

Notes

of the freedom of speech and expression, to the invasion of privacy, and to the disproportionate severity of penalization for offences that are placed on crimes committed in cyberspace compared to crimes committed in the hear and now.

Sadly, this is true to a large extent given the clunky treatment of ―cyber terrorism, the intolerable pre-censorship that is enabled by the blocking of websites, the broad approach to the monitoring and collection of data, and the demanding obligations of intermediaries to cooperate with interception, monitoring and decryption of data for poorly defined reasons.

- While our Constitution's fundamental rights chapter, which enshrines certain basic, democratic, and profound rights, might not have the same vocabulary of due process as we see in the US, it nevertheless requires restrictions to be reasonable. Precedents and the wider jurisprudence in the field have further developed the concepts of checks and balances, procedural safeguards and legitimacy of restraints that a functioning democracy like India must accord to its people. It can be argued that several provisions of the ITA cause significant tension with the right to freedom of speech and expression, the right against self- incrimination, the right to equality before the law, and the right to practice a trade or profession.

2.10 Pre-censorship

Some of the most excessive provisions relate to the free hand with which public access to websites can be blocked. Previously, there was some hope that the rules yet to be formulated in connection with section 69-A would offer some procedural safeguards. The recently notified rules do contain details – in the bureaucratese that we have come to expect – of the process to be followed by the designated functionaries. They also permit the concerned person or intermediary to submit a reply and clarifications to the committee before the decision to block access is taken.

These rules are to a large extent undermined by rule 9 (Blocking of information in cases of emergency'), which provides that, 'in any case of an emergency nature, for which no delay is acceptable'', the process will turn into an internal escalation within the department of IT and interim directions relating to blocking access may be issued without giving (him) an opportunity of hearing. There are those who think that, given the events of 26/11, this is wholly justified but the prospect of abuse fills others with dread. The rules may offer detailed time- frames within which orders are made and approved, require reasons to be recorded in writing, provide that emergency orders may be revoked and information unblocked, etc. Regardless, the nature of the process

(executive rather than judicial), the ease with which it can be abused, and the fact that the review committee will only meet once in two months to check for compliance, set aside incorrect orders and unblock information, does not offer much comfort. If a site is incorrectly blocked, it could take up to two months for this to be rectified, which could cause a great damage to the owner of the site, and indeed to the wider public that has an interest in uncensored, free speech.

Given that any person can submit a request, it is not unreasonable to anticipate a certain level of frivolous and malicious requests for blocking sites, especially given that the grounds for blocking are very wide (the often repeated set that we are familiar with, namely, in the interest of sovereignty and integrity of India; relating to defence of India/ security of State/ friendly relations with foreign states/ public order and for preventing incitement to commission of any cognizable offences). Without a review committee constantly monitoring and policing the unbridled use of the provisions, the backlog of blocking decisions that may need to be reversed can become a mountain very quickly. The dangers of pre-censorship and the curtailment of dialogue, debate and free speech are even greater in a country with an increasingly thin-skinned populace. Faced with a volatile backdrop of great diversity of religion, political opinions, views on sexuality, morality, obscenity and other highly subjective values and beliefs, there is immense extra-legal pressure on free speech. Thus, there is now a need for greater vigilance so that the thought police do not wield the stick of harsh penalties under the ITA without reason and due process.

2.11 Privacy and surveillance

This topic pulls together concerns around the blanket monitoring and collecting of traffic data or information, the interception and decryption (under duress) by intermediaries (now a large superset of ISPs, search engines, cyber cafes, online auction sites, online market places, etc.) and the wide definition of ―cyber terrorism (which ludicrously even casts defamation as a terrorist activity).

Some of the broad concerns in relation to interception, monitoring and decryption in (section 69) are that:

- There is no provision for a clear nexus between an intermediary and the information or resource sought to be monitored or intercepted,
- The usual internationally recognised exception to liability where an intermediary operates purely as a conduit and has no control over data flowing through its network is not clearly spelt out,
- The penalties for non-cooperation are extremely harsh, especially given the absence of (a) and (b) above,

Notes

- These onerous penalties can be said to be in violation of Article 14 as they seem entirely disproportionate. Similar offences and remedies in the Code of Criminal Procedure or the Indian Penal Code prescribe less severe penalties, by an order of magnitude in fact. When the only difference between the offences is the medium in which information is contained, it seems arbitrary to impose a much harsher punishment on an online intermediary than on a member of the public who, for example, furnishes false information to the police in connection with a trial or enquiry.
- The rules made in relation to monitoring, interception and decryption, offer some procedural safeguards, in that they impose a time limit on how long a directive for interception or monitoring can remain in force, a ceiling on how long data can be kept before it is required to be destroyed, etc. However, the effect of these is greatly diluted by exceptions for functional requirements', etc. The astonishing irony is that rule 20 requires the intermediary to maintain 'extreme secrecy'' and 'utmost care and precaution'' in the matter of interception, monitoring or decryption of information 'as it affects the privacy of citizens'' In a similar vein, there are concerns around the monitoring and collection of traffic data (Section 69B) as the section contains an unreasonably long list of grounds for monitoring. These include such extreme excesses as forecasting of imminent cyber incidents', monitoring network application with traffic data or information on computer resource', identification and determination of viruses/computer contaminant', and the catch-all any other matter relating to cyber security'.

Finally, the main criticism of the ITA approach to ―cyber terrorism is the very wide net that it seeks to cast, looking for a game that has little or nothing to do with the named offence. Amongst the cast of creatures unwittingly caught during this fishing expedition, we find some unlikely victims. In addition to the usual grounds of offence against sovereignty, national security, defence of India, etc., which we have seen in relation to other sections, the ITA considers the following as acts of cyber terrorism – broadly speaking, unauthorized access to information that is likely to cause:

- Injury to decency,
- Injury to morality,
- Injury in relation to contempt of court, and
- Injury in relation to defamation.

This would almost be laughable if these grounds were not enacted into law, posing a threat to civil liberties by their very existence. Other countries have some notion of political ideology, religious case, etc. in their view of terrorism. That (a) to (d) above

have been shoehorned into a clause that imposes the stiffest penalty within the entire ITA (life imprisonment) gives even more cause for concern.

2.12 Civil Liability for Corporate

Notes

As mentioned above, anybody corporate who fail to observe data protection norms may be liable to pay compensation if:

- It is negligent in implementing and maintaining reasonable security practices, and thereby
- Causes wrongful loss or wrongful gain to any person;

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act.

2.13 Adjudication

Having dealt with civil offences, the Act then goes on to describe civil remedy to such offences in the form of adjudication without having to resort to the procedure of filing a complaint with the police or other investigating agencies. Adjudication powers and procedures have been elaborately laid down in Sections 46 and thereafter. The Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. If at all one section can be criticized to be absolutely lacking in popularity in the IT Act, it is this provision. In the first ten years of existence of the ITA, there have been only a very few applications made in the nation, that too in the major metros almost all of which are under different stages of judicial process and adjudications have been obtained in possibly less than five cases. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages.

This section should be given much popularity and awareness should be spread among the public especially the victims of cybercrimes and data theft that such a procedure does exist without recourse to going to the police and filing a case . It is time the state spends some time and thought in enhancing awareness on the provision of adjudication for civil offences in cyber litigations like data theft etc. so that the purpose for which such useful provisions have been made, are effectively utilized by the litigant public.

There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level, has also been described in the Act. Every

adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure.

Notes

2.14 Evidences

Evidences are a major concern in cybercrimes. Pat of evidences is the ―crime scene issues. In cybercrime, there is no cybercrime. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Very often, nothing could be seen as a scene in cybercrime. The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. While filing cases under IT Act, be it as a civil case in the adjudication process or a criminal complaint filed with the police, many often, evidences may lie in some system like the intermediaries computers or some times in the opponent's computer system too. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc.) since most of the computer history and log files are volatile in nature.

There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required. For this there are software tools like―Encase with a global recognition and our own C-DAC tools which are available with much retrieval facilities, search features without giving any room for further writing and preserving the original version with date stamp for production as evidence. Rehabilitation

2.15 Misuse of technology

When the complaint itself does not make out criminal case to issue the process, to force the accused to undergo trial would be clear misuse of the process of the Court and this should not be allowed. The Additional Sessions Judge while rejecting the revision application dealt with the liability of the contractor on the basis of terms of the contract and the cheque. The learned counsel for the respondent also contended that the matter was referred to arbitrator and arbitrator also held that the contractor is liable to pay on

the basis of that cheque. As far as civil liability of the contractor/petitioner is concerned, it is not necessary to look into the same in present matter.

2.16 Constitutional validity of section 66A of IT Act85

Notes

It said the court cannot pass an order for banning all arrest in such cases as operation of section 66A (pertaining to objectionable comments) of the Information Technology Act has not been stayed by the apex court which is examining its constitutional validity.

The advisory issued by the Centre says that, State governments are advised that as regard to arrest of any person in complaint registered under section 66A o f the Information Technology Act, the concerned police officer of a police station may not arrest any person until she/he has obtained prior approval of such arrest from an officer, not below the rank of inspector general of police (IGP) in metropolitan cities or of an officer not below the rank of deputy commissioner of police (DCP) or superintendent of police (SP) at district level, as the case may be.' In fact, section 66A of IT Act is a potential tool in the hands of rulers to curtail the voice of opposition. It is fatal for the freedom of speech of netizens in general and the press in particular.

The Indian Penal Code and other provisions of the IT Act, especially after the 2008 amendment, provide enough safeguards against defamation, intentional insult leading to breaking the peace, incitement to commit offence, etc. Political criticism always causes some annoyance to someone. Ruling party and Opposition members routinely say unflattering things about each other. Should they be charge sheeted, too? The basic idea behind freedom of speech is to allow divergent critical views without looking into whether people are annoyed or inconvenienced.

Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Art. 19(1)(a) of our Constitution. The fact that some information is "grossly offensive" (s.66A(a)) or that it causes "annoyance" or "inconvenience" while being known to be false (s.66A(c)) cannot be a reason for curbing the freedom of speech unless it is directly related to decency or morality, public order, or defamation (or any of the four other grounds listed in Art. 19(2)). It must be stated here that many argue that John Stuart Mill's harm principle provides a better framework for freedom of expression than Joel Feinberg's offence principle. The latter part of s.66A(c), which talks of deception, is sufficient to combat spam and phishing, and hence the first half, talking of annoyance or inconvenience is not required. Additionally, it would be beneficial if an explanation could be added to s.66A(c) to make clear what "origin" means in that section. Because depending on the construction of that word s.66A(c) can, for instance, unintentionally prevent organisations from using proxy servers, and may prevent a person from using a sender envelope different from the "from" address in an

Notes

e-mail (a feature that many e-mail providers like Gmail implement to allow people to send mails from their work account while being logged in to their personal account). Furthermore, it may also prevent remailers, tunneling, and other forms of ensuring anonymity online. This doesn't seem to be what is intended by the legislature, but the section might end up having that effect. This should hence be clarified.

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

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

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

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

A large part of s.66A can be traced back to Section 10(2) of the UK's Post Office (Amendment) Act, 1935: If any person —

(a) sends any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character; or

(b) sends any message by telephone, or any telegram, which he knows to be false, for the purpose of causing annoyance, inconvenience, or needless anxiety to any other person; or

(c) persistently makes telephone calls without reasonable cause and for any such purposes as aforesaid; he shall be liable upon summary conviction to a fine not exceeding ten pounds, or to imprisonment for a term not exceeding one month, or to both such fine and imprisonment.

Section 66A bears a striking resemblance to the three parts of this law from 1935, with clauses (b) and (c) being merged in the Indian law into a single clause (b) of s.66A,

with a whole bunch of new "purposes" added. Interestingly, the Indian Post Office Act, 1898, was never amended to add this provision.

The differences between the two are worth exploring.

Notes

Term of Punishment

The first major difference is that the maximum term of imprisonment in the 1935 Act is only one month, compared to three years in s.66A of the IT Act. It seems the Indian government decided to subject the prison term to hyper-inflation to cover for the time. If this had happened for the punishment for, say, criminal defamation, then that would have a jail term of up to 72 years! The current equivalent laws in the UK are the Communications Act, 2003 (s. 127) and the Malicious Communications Act 1988 (s.1) for both of which the penalty is up to 6 months' imprisonment or to a maximum fine of £5000 or both. What's surprising is that in the Information Technology (Amendment) Bill of 2006, the penalty for section 66A was up to 2 years, and it was changed on December 16, 2008 through an amendment moved by Mr. A. Raja (the erstwhile Minister of Communications and IT) to 3 years. Given that parts of s.66A(c) resemble nuisance, it is instructive to note the term of punishment in the Indian Penal Code (IPC) for criminal nuisance: a fine of ₹ 200 with no prison term. "Sending" vs. "Publishing"

J. Sai Deepak, a lawyer, has made an interesting point that the IT Act uses "send" as part of its wording, and not "publish". Given that, only messages specifically directed at another would be included. While this is an interesting proposition, it cannot be accepted because: (1) even blog posts are "sent", albeit to the blog servers—s.66A doesn't say who it has to be sent to; (2) in the UK the Communications Act 2003 uses similar language and that, unlike the Malicious Communication Act 1988 which says "sends to another person", has been applied to public posts to Twitter, etc.; (3) The explanation to s.66A(c) explicitly uses the word "transmitted", which is far broader than "send", and it would be difficult to reconcile them unless "send" can encompass sending to the publishing intermediary like Twitter. Part of the narrowing down of s.66A should definitely focus on making it applicable only to directed communication (as is the case with telephones, and with the UK's Malicious Communication Act), and not be applicable to publishing. Section 66A(c) Section 66A(c) was also inserted through an amendment moved by Mr. Raja on December 16, 2008, which was passed by the Lok Sabha on December 22, 2008, and a day after by the Rajya Sabha. (The version introduced in Parliament in 2006 had only 66A (a) and (b).) This was done in response to the observation by the Standing Committee on Information Technology that there was no provision for spam. Hence it is clear that this is meant as an anti-spam provision. However, the careless phrasing makes it anything but an anti-spam provision. If instead of "for the purpose of causing annoyance or inconvenience or to deceive or to mislead

Notes

the addressee or recipient about the origin of such messages" it was "for the purpose of causing annoyance and inconvenience and to deceive and to mislead the addressee or recipient about the origin of such messages", it would have been slightly closer to an anti-spam provision, but even then doesn't have the two core characteristics of spam: that it be unsolicited and that it be sent in bulk. (Whether only commercial messages should be regarded as spam is an open question.) That it arise from a duplicitous origin is not a requirement of spam (and in the UK, for instance, that is only an aggravating factor for what is already a fine-able activity). Curiously, the definitional problems do not stop there, but extend to the definitions of "electronic mail" and "electronic mail message" in the 'explanation' as well. Those are so vast that more or less anything communicated electronically is counted as an e-mail, including forms of communication that aren't aimed at particular recipients the way e-mail is.

Hence, the anti-spam provision does not cover spam, but covers everything else. This provision is certainly unconstitutional.

Section 66A (b)

Section 66A(b) has three main elements: (1) that the communication be known to be false; (2) that it be for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will; (3) that it be communicated persistently. The main problem here is, of course, (2). "Annoyance" and "inconvenience", "insult", "ill will" and "hatred" are very different from "injury", "danger", and "criminal intimidation". That a lawmaker could feel that punishment for purposes this disparate belonged together in a single clause is quite astounding and without parallel (except in the rest of the IT Act). That's akin to having a single provision providing equal punishment for calling someone a moron ("insult") and threatening to kill someone ("criminal intimidation"). While persistent false communications for the purpose of annoying, insulting, inconveniencing, or causing ill will should not be criminalised (if need be, having it as a civil offence would more than suffice), doing so for the purpose of causing danger or criminal intimidation should. However, the question arises whether you need a separate provision in the IT Act for that. Criminal intimidation is already covered by ss. 503 and 506 of the IPC. Similarly, different kinds of causing danger are taken care of in ss.188, 268, 283, 285, 289, and other provisions. Similarly with the other "purposes" listed there, if, for instance, a provision is needed to penalize hoax bomb threats, then the provision clearly should not be mentioning words like "annoyance", and should not be made "persistent". (At any rate, s. 505(1) of the IPC suffices for hoax bomb threats, so you don't need a separate provision in the IT Act).

I would argue that in its current form this provision is unconstitutional, since there is no countervailing interest in criminalising false and persistent "insults", etc., that will

allow those parts of this provision to survive the test of 'reasonableness' under Art.19(2). Furthermore, even bits that survive are largely redundant. While this unconstitutionality could be cured by better, narrower wording, even then one would need to ensure that there is no redundancy due to other provisions in other laws.

Section 66A(a)

In s.66A(a), the question immediately arises whether the information that is "grossly offensive" or "menacing" need to be addressed at someone specific and be seen as "grossly offensive" or "menacing" by that person, or be seen by a 'reasonable man' test.

Additionally, the term "grossly offensive" will have to be read in such a heightened manner as to not include merely causing offence. The one other place where this phrase is used in Indian law is in s.20 (b) of the Indian Post Office Act (prohibiting the sending by post of materials of an indecent, obscene, seditious, scurrilous, threatening, or grossly offensive character). The big difference between s.20 (b) of the IPO Act and s.66A of the IT Act is that the former is clearly restricted to one - to-one communication (the way the UK's Malicious Communication Act 1988 is). Reducing the scope of s.66A to direct communications would make it less prone to challenge.

2.17 Criminalization of Online Speech and Social Media87

The criminalization of online speech in India is of concern as the authorities have prosecuted legitimate political comment online and personal views expressed on social media. New free speech opportunities offered by social media usage in India have been diminished after the introduction of provision 66A of the IT Act and the arrest of a number of Indian citizens for posting harmless content. This chapter looks at how Section 66A constitutes a significant impediment to freedom of expression and will demonstrate the need to reform the law.

In 2011, Communications Minister Kapil Sibal asked Google, Facebook and Yahoo! to design a mechanism that would pre-filter inflammatory and religiously offensive content. This request was not just, as noted at the time, technologically impossible, it was also a clear assault on free speech. The request demonstrated that even if Section 66A were reformed, further work would still be needed to prevent politically motivated crackdowns on social media usage.

Section 66A of the IT Act is both overly broad and also carries a disproportionate punishment. The section punishes the sending of any information that is grossly offensive or has menacing character' or any information meant to cause annoyance, inconvenience, obstruction, insult, enmity, hatred or ill will, among other potential grievances. The provision carries a penalty of up to three years imprisonment and a fine.

2.18 Recent Cases

Notes

The petition was also filed regarding the arrest of a Hyderabad-based woman activist, who was sent to jail over her Facebook post in which certain objectionable' comments were made against Tamil Nadu Governor K Rosaiah and Congress MLA Amanchi Krishna Mohan. After filing of the petition, she was released by a district court at Hyderabad.

Jaya Vindhayal, the state general secretary of People's Union for Civil Liberties (PUCL), was arrested on May 12 under section 66A of the IT Act for the objectionable' post. According to the police; she had also allegedly distributed pamphlets making objectionable allegations against Rosaiah and Mohan before posting the comments online.

The matter was mentioned before the bench by law student Shreya Singhal, seeking an urgent hearing in the case, saying the police is taking action in such matters even though a PIL challenging validity of section 66A is pending before the apex court.

She had filed the PIL after two girls – Shaheen Dhada and Rinu Shrinivasan – were arrested in Palghar in Thane district under section 66A of IT Act after one of them posted a comment against the shutdown in Mumbai following Shiv Sena leader Bal Thackeray's death and the other —liked it. On November 30, 2012, the apex court had sought response from the Centre on the amendment and misuse of section 66A of IT Act and had also directed the Maharashtra government to explain the circumstances under which the 21-year-old girls were arrested.

Pursuant to the notice issued by the apex court, the Centre had informed it that the controversial provision in the cyber law under which two girls were arrested for Facebook comments did not curb freedom of speech and alleged high handedness' of certain authorities did not mean that it was bad in law.

2.19 Case Study: Facebook Arrests

On Sunday 18 November 2012, a 21-year-old Mumbai woman, Shaheen Dhada, shared her views on Facebook on the shutdown of the city as Shiv Sena chief Bal Thackeray's funeral was being held. Her friend Renu Srinivasan liked' her post.

At 10.30 am the following day, they were both arrested and were ordered by a court to serve 14 days in jail. Hours later, they were eventually allowed out on bail after paying two bonds of ₹ 15,000 (£145) each Dhada had posted, Respect is earned, not given and definitely not forced. Today Mumbai shuts down due to fear and not due to respect'. A local Shiv Sena leader filed a police complaint and Dhada and Srinivasan were booked under Section 295 A of the Indian Penal Code

(IPC) for deliberate and malicious acts, intended to outrage religious feelings or any class by insulting its religion or religious beliefs.' Subsequently they were also

charged under Section 505 (2) of the IPC for making statements creating or promoting enmity, hatred or ill-will between classes', and the police added Section 66A of the IT Act to the list of charges.

Notes

This should not be seen merely as social media regulation', but as a restriction on freedom of speech and expression by both the law and the police. Section 66A makes certain kinds of speech-activities (causing annoyance') illegal if communicated online, but legal if that same speech-activity is published in a newspaper. Finally, this is similar to the Aseem Trivedi case where the police wrongly decided to press charges and to arrest.

This distinction is important as it being a Facebook status update should not grant Shaheen Dhada any special immunity; the fact of that particular update not being punishable under s.295 or s.66A (or any other law) should :

- Section 64 of the IT Act is about recovery of penalty' and the ability to suspend one's digital signature if one doesn't pay up a penalty that's been imposed.
- The police generally cannot, without a warrant, arrest a person accused of a bailable offence unless it is a cognizable offence. A non-bailable offence is one for which a judicial magistrate needs to grant bail, and it isn't an automatic right to be enjoyed by paying a bond-surety amount set by the police.
- Section 295A of the IPC has been held not to be unconstitutional. The first case to challenge the constitutionality of section 66A of the IT Act was filed recently in front of the Madurai bench the Madras High Court.)
- One can imagine an exceptional case where such an act could potentially be defamatory, but that is clearly exceptional.
- This is entirely apart from the question of how the Shiv Sena singled in on Shaheen Dhada's Facebook comment.

2.20 Rights vs. Responsibilities

There is also a trend visible that business interest are increasingly protected for the reason of copyright by developed countries, with freedom of expression and free flow of information sacrificed.

Freedom of expression needs to be promoted with legitimate limitations and in balance with other digital rights within an expanded legal and regulatory framework. There are challenges to deal with liability of intermediaries and governmental surveillance which might undermine freedom of expression.

The ubiquity of the technology goes hand-in-hand with the ubiquity of social media. But with rights come responsibilities. Unchecked, social media can also allow

Notes

disinformation, slander, racism, incitement to hatred, victimization and a catalogue of ills, some – obviously – more serious than others.

If something incites violence or racism, then it should be prosecuted, regardless of whether it is said in front of physical people or their virtual avatars. But drawing this line is no easy matter.

Is there a need for a regulatory authority with powers to ban/suspend coverage of objectionable material? If yes, should the regulatory authority be self-regulatory or should it have statutory powers?

As our submission restricts itself to the matter of objectionable content on the Internet, we will not comment on the possible need for a regulatory authority for the print and electronic media. However, we believe that it will be wholly inappropriate to grant a regulatory authority with powers to ban/suspend coverage of objectionable material on social media and on the Internet more broadly, be this self-regulatory authority or one with statutory powers.

For one thing, such a move would erroneously elide the distinction between traditional media and the speech of ordinary people on social media as it would by default treat their role in society and the weight of their speech acts as the same. As explained above, where censorship is considered, the facts of the situation should always be assessed against clearly defined thresholds. These thresholds include the extent or reach of the speech and the likelihood or probability of action in response to the speech – apart from the severity, intent, content, imminence and context. In the large majority of cases, the impact of the speech of ordinary individuals will not be the same as that of mainstream media when assessed according to these criteria.

Indeed, it is important to also remember that where social media is concerned, it is the users, not the platform owners, who are the authors of the messages. In other words, Internet intermediaries such as Facebook, Twitter and Word Press, on which ordinary people rely to publish their messages, are fundamentally different from traditional media: while traditional media produces content, Internet intermediaries are merely messengers, much as telecommunication companies are of voice messages delivered over landlines and mobile phones. Although a regulatory authority would inevitably require the cooperation of Internet intermediaries to be effective, its prime targets would thus have to be ordinary people. Such non-judicial regulation of the speech of ordinary people is wholly inappropriate in a democratic country.

Indeed, as explained above, while there may be content on the Internet that is seen as socially objectionable, much of it is not objectionable in the legal sense by any means. However, the determination of whether or not a specific set of facts violates the law can only be made by the judiciary or by an independent body that is free of political,

Notes

commercial and other unwarranted influences. Where discretionary powers are given to the authorities to make such assessments, this is all too likely to lead to misuse, further contributing to a chilling effect that already exists, as India's citizens increasingly start to censor themselves.

The establishment of a regulatory authority thus will likely substantially undermine the empowering effect that the Internet has had for ordinary people, and in particular for the boost it has given to their abilities to express themselves on a wide range of issues that concern them. While this includes speech that is at times of a questionable nature, it also lead to a great number of benefits, including forcing greater transparency and accountability on a wide range of power centers in our country, be they political or commercial. If these buds of active citizenship that so many Indians have embraced enthusiastically are to flower, freedom of expression should be protected and promoted by all means possible, rather than curtailed.

This is in addition to the fact that, as experiences in a wide range of countries has shown, filtering the Internet or creating a blacklist of undesirable sites to be made inaccessible are by no means effective measures. While generally merely driving the consumption of the material that was sought to be banned underground, rather than stopping it, such measures tend to cause content that would be wholly legitimate to be blocked as well. This can be both as a consequence of human mistakes (as humans not trained for this task interpret definitions overly broad, as we have seen repeatedly in the context of the implementation of section 66A) or of technical limitations (as filter systems based on key words will filter out all content containing those key words, without considering at their intent or context).

This is not to say, of course, that action should not be taken against speech that clearly violates the law. However, several mechanisms to do so are already in place – and this in addition to the legal right every Indian has to approach the Courts.

For example, section 69A of the IT Act makes it possible for the Central Government to block content in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above'. Importantly, the Rules that were issued under the section explicitly allow for a speed procedure to put into place such blocks in case of emergency.

At the same time, the Intermediary Guidelines Rules, issued in 2011 under section 79 of the IT Act, make it possible for any Indian to send a take-down request to an intermediary for content that they believe violates the Rules.

Like section 66A, the Intermediary Guidelines Rules unfortunately suffer from important procedural and substantive shortcomings that have been argued to have a

Notes

chilling effect on freedom of speech and expression, and strong protections of freedom of expression on the Internet in India would require these Rules, too, therefore to be revised extensively. For example, one aspect of the Intermediary Guidelines Rules that has come in for heavy criticism is that the Rules have effectively privatized censorship by relying on the intermediaries to make the assessment as to whether or not content is unlawful, rather than requiring the judiciary or an independent body to do so. We have repeatedly pointed to the dangers of doing so in this submission.

However, the principle that intermediaries should take down unlawful content stands by and large undisputed in the country. Rather than establishing a regulatory authority, a review of the Intermediary Guidelines Rules can thus be used as an opportunity to devise a mechanism that protects free speech while also effectively dealing with illegal content on the Internet in India as required. Such a mechanism would need to include at the very minimum judicial intervention or review at some point in the process if content is to be removed, as well as recognition of the author's right to be informed and right to object/appeal.

In addition to such a review, there is however one more area where far greater energy could be focused: that of non-legal measures to fight objectionable speech online. Where objectionable content on the Internet is discussed, the tendency in India has been to overwhelmingly to look at censorship and arrests as ways to fight such speech. Yet especially in a country with the diversity of India - where what might be offensive to one community might be common sense to another – such an approach alone is clearly never going to fully resolve the problem of objectionable speech. As there is a considerable gap between speech that is socially unacceptable and that which is legally unacceptable, the singular focus on the law will inevitably leave many types of speech uncontested. But perhaps more importantly, as it fosters a culture of intolerance, such a purely legal approach might also have severe negative repercussions for the social fabric in the long-term.

What we need, therefore, is a far more extensive toolbox, containing positive measures as well that are geared towards nurturing public discussion and a culture of tolerance, and, ultimately, changing social behavior on the Internet.

Such a toolbox should contain, among other things, both education for school children and public awareness campaigns about the ways in which Indians fundamental rights and concomitant obligations translate to the Internet; about the damage hate speech and other forms of objectionable speech do to the social fabric of the country; and about the ethical actions all of us can take when we observe abuse and other forms of objectionable content.

Notes

It should also involve the active use of counter-speech and social dialogue, including through the public denouncement of instances of hate speech by public officials. It deserves consideration, for example, whether, when people from the North East started to flea Bangalore in mid-August 2012 following the spread of rumors that they would be attacked as a fall-out from violence that had occurred in Assam, a public announcement of the then Prime Minister on national television that the government would not allow this to happen would not have been more effective than the blocking of Internet content at the time when the number of people fleeing had already substantially come down. The explicit rejection of acts of abuse and other objectionable speech by community leaders and other influential figures can go a long way in stemming the flow and impact of such content indeed.

All these measures would provide considerable fill-up to the wide range of non-legal strategies that Internet users in India are already developing to fight objectionable content online. For example, in Don't Let it Stand! An Exploratory Study of Women and Online Abuse in India', conducted in 2012-2013 by the Internet Democracy Project, women users of social media highlighted support from their online community, not the law, as one of the most critical factors to ensure their fight against online abuse was successful. Where they were alone and isolated, it was difficult for them to respond. Where others in their circle supported them actively, the likelihood that they were able to deal with an abuser effectively immediately increased many-fold. Non-legal initiatives by the government, the media, schools, not-for-profit organisations, religious and caste associations and a slew of other groups could thus do much to further empower users to deploy such strategies to fight abuse and hate speech.

What all these non-legal measures to address objectionable content online have in common, is that they rely on freedom of speech and expression, rather than on restrictions on this right, to combat objectionable content. Indeed, as we have pointed out also at the beginning of our submission, it is important to remember that overall, freedom of expression facilitates the exercise of other human rights. Fighting against hate speech, or for equality, and strengthening freedom of expression are, thus, not simply compatible with each other. Instead, they exist in an affirming, mutually reinforcing relationship as they make complementary yet essential contributions to the securing and safeguarding of human dignity.

Currently, unfortunately, initiatives that recognize this interplay are sorely lacking in India. Rather than towards establishing a social media regulator, it is towards initiatives such as these that a great part of our energies should urgently be devoted.

Notes

2.21 Misuse of Social Media and Freedom of Speech and Expression

Indeed, as explained above, while there may be content on the Internet that is seen as socially objectionable, much of it is not objectionable in the legal sense by any means. However, the determination of whether or not a specific set of facts violates the law can only be made by the judiciary or by an independent body that is free of political, commercial and other unwarranted influences. Where discretionary powers are given to the authorities to make such assessments, this is all too likely to lead to misuse, further contributing to a chilling effect that already exists, as India's citizens increasingly start to censor themselves.

2.22 Summary

The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law Information Technology Act 2000. Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. The increase rate of technology in computers has led to enactment of Information Technology Act 2000.

The ITA has sought to address and improve aspects such as technology neutrality, data protection, phishing and spam, child pornography, the liability of intermediaries and cyber terrorism. While many of these amendments are a step in the right direction, the actual drafting that implements the high level objectives suffers in many respects. The current law is a bit of an abnormal document in that it contains elements of both concepts, which some attention to detail could easily have averted.

Social media offers huge opportunities for freedom of expression. Individuals are able to see their thoughts traverse the globe in an instant; news – and its interpretation – is not automatically dependent on the filtering process of the media, or of government. The freedom of expression on Internet is a crucial challenge to address in formulating inclusive information society.

2.23 Review Questions

1. Discuss section-66 and section-67 in detail.
2. What are the different sections of IT Act, 2000 which deals with offences?
3. What are the criminal liabilities for misusing information technology?

4. What do you mean by offences? Discuss in context of IT Act, 2000.
5. Describe some case laws of privacy and pornography.
6. Discuss the concept of accrued liability and procedural law.
7. Explain ―data protection in detail.
8. What do you mean by privacy and surveillance?
9. What are the civil liabilities for corporates? Discuss.
10. Describe the term ―pre-censorship.
11. Explain difference between rights and responsibilities?
12. Discuss some consequences of section 66A.
13. What do you understand by sending and publishing?
14. Discuss Facebook case study of Shaheen Dhada.
15. How freedom of speech and expression performs in social media?

Notes

2.24 Further Readings

- A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime
- Introduction to Indian Cyber Law by Rohas Nagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf
- Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
- Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
- Cyber Forensics in India; retrieved from http://perry4law.org/cfii/
- Digital Evidence & the Indian Law by Asian School of Cyber Laws; retrieved from http://www.asianlaws.org/del.pdf

UNIT–3

Notes

E-Commerce and Laws in India

(Structure)

3.1 Learning Objectives

After studying the chapter, students will be able to:

- Discuss the online Defamation;
- Describe the problems in applying traditional methods;
- Discuss the misuse of cyber world in terms of defamation;

- Explain the Human Rights related with Cyber Space;
- Describe the Constitutional Mandate;
- Discuss the Information Technology and the law of privacy related;
- Describe the misuse of privacy and human rights.

Notes

3.2 Introduction

The Tort of Cyber Defamation is considered to be the act of defaming, insulting, offending or otherwise causing harm through false statements pertaining to an individual in cyberspace. This is commonly done through the Internet via websites, blogs, forums, emails and instant messaging, chat rooms and now in the social networking sphere. Defamation law in general describes the tort as the issuance of a false statement about another person, which causes that person to suffer harm' (Larson) where libel is the written form and slander is spoken. Libel is typically the form addressed with cyber defamation because the Internet essentially receives the same protections as print and published media. The other elements applied to defamation include:

- The unprivileged publication of the statement to a third part.
- If the defamatory matter is of public concern, fault amounts at least to negligence on the part of the publisher
- Perceivable damage to the plaintiff

Along with the core elements of defamation, the burden of proof is placed on the plaintiff in a case, damages are usually awarded monetarily and in the United States, truth is an absolute defense.

Cyber or online defamation is considered to be as, if not more harmful than defamation in the form of libel and slander in the brick and mortar, physical world. In some cases, the effects of online defamation could be exponentially worse than an offline incident due to the global nature of the Internet and the fact that the statements can be accessed by virtually anyone. In addition to this, the issue of anonymity online raises even more concern when dealing with defamation because the author or origin of the statements may be very difficult to trace depending on the medium.

However, in India Defamation is the intentional infringement of another person's right to his good name. Cyber defamation is anything which could be seen, read or heard with the help of computers. It is the wrongful, intentional publication of words or behavior concerning another person, which has the effect of injuring that person's status or good name or reputation in society. When cyber defamation is concerned, number of people who may view the comment may be gigantic. It can be more effective when

Notes

posted in a specific newsgroup. Section 499 of the Indian Penal Code, 1860 discusses Defamation. Not many people are aware of how easily a defamation action can arise and it is this ignorance or lack of awareness which increases the risk of defamation over the internet. However, the courts have held that there will be no publication unless the third party to whom the defamatory statements were made actually understands their meaning.

The following are among the areas of risk of exposure to online defamation:

- World Wide Web
- Discussion groups
- Intranets
- Mailing lists and bulletin boards
- E-mail

Defamation cases involving the internet generally fall into two basic categories:-

1. Cases involving the liability of the primary publishers of the defamatory material, e.g. web site content providers, e-mail authors etc.; and
2. Cases involving the liability of the internet service providers or bulletin board operators.

The ease of publishing information, correct or not, to millions of listeners worldwide over the internet has caused defamation to become an increasing problem. For example, one of the newest types of web sites on the internet are suck sites', web sites that use a domain name that includes the name or the trademark of a company and then contains the information critical of that company. Such sites go beyond just publishing negative comments about an individual or company and actively establish a specific web site with an identifiable name such as lucentsucks.com. A key question in this area is what remedies does the law provide to the victims of such actions?

Public Privacy is about fundamental flexibility and privacy rights grounded in global human rights law. Cyberspace is a borderless public space in which nationals, paying little respect to their citizenship, nationality, ethnicity, political introduction, sexual orientation or overall foundation convey and associate.

Through new innovations, Cyberspace offers an environment that comprises of numerous members with the capacity to influence and impact one another. This space is transparent and nonpartisan in its tendency however frequently characterized, expanded, restricted and blue-penciled by individuals who make utilization of it. Correspondence through the internet is consequently regularly unknown but utilized and imparted to an overall wide public, which stays, to the expansive part; generally obscure for the individual internet client, to be specific us. All things considered, we do impart some

of our most private and individual data with this unknown crowd. This overall public records today around 2.5 billion internet users. In the event that cyberspace were a nation, it would be the biggest and most populated nation on the planet, yet without any government, administrative bodies, law implementation, insurance instrument, or tenets for investment, not to mention anything that verges on a 'digital constitution' for all internet-nationals.

By imparting private information, billions of internet users have effectively made virtual twins in this new space, while never having an opportunity to erase information. Personal connections and 'being friends' through social networks, for example, Renren and Facebook can be nameless on the one side, but give an endless measure of personal information and private messages. People's private and additionally expert lives are publically moving in cyberspace. Organizations and endeavors, instruction and preparing, accounts and money matters, private correspondence, and even wellbeing and personal issues are presently by offering private information, billions of internet users have officially made virtual twins in this new space, while never having an opportunity to erase information. Personal connections and 'being friends' through social networks, for example, Renren and Facebook can be nameless on the one side, but give a limitless measure of personal information and private messages. People's private and in addition expert lives are publically moving in cyberspace. Organizations and undertakings, training and preparing, funds and mass trading, private correspondence, and even wellbeing and personal issues are presently managed by any individual who looks for access to it in this 'unending' space.

The vehicle by which information moves in this space is the internet and it precedes onward the interstate called World Wide Web. However apparently to national space and domain that we call a nation or an express, the way people and on-screen characters act and settle on choices in this space is guided through principles and standards generally recorded in constitutions or laws.

On account of Cyberspace, these citizens are internet users all as far and wide as possible. Albeit international governmental associations (IGOs), for example, the UN, the Organization for American States, the African Union or the European Union, plan to set international principles for the utilization of cyberspace and internet to be regarded and authorized by national governments, they for the most part neglect to do so. The purpose behind this is that states' powers and requirement systems frequently end at state borders on the grounds that their order to ensure human rights is completely focused around state sovereignty and governments. IGOs and international courts regularly likewise have just constrained measures and intends to ensure human rights, not to mention implement them.

Notes

Since cyberspace has no physical or national borders, the methods and approaches to represent this new borderless administration are not yet characterized. In any case, in the level headed discussion and exertion to set up a cyberspace legislation administration, human rights standards and principles, (for example, the human rights to protection, security, wellbeing, free declaration, development and ventur(e) offer direction to the different number of diverse performers that are included in the outline of the cyberspace administration and how to conceivably control it. If at any time built, the cyberspace administering body will be one of different stakeholders and on-screen characters including national, international and additionally private performing artists, for example, agents of organizations, social networks, NGOs and people.

3.3 Online Defamation

Defamation is a statement that harms the reputation of someone else. Courts have to balance the reputation of one person with the free speech rights of the other. Statements have to be repeated to at least one third person and must have caused damage. There are two forms of defamation: libel and slander. Libel involves the publishing of a falsehood that harms someone. Slander is the same doctrine applied to the spoken word. Collectively, they are referred to as defamation. Both fall under the jurisdiction of individual states, which usually require the falsehood to be intentional.

The common law tort of defamation provides a legal remedy to those injured by gossip. Specifically, an individual is subject to liability if he or she damages another person's reputation by speaking or publishing false statements about that person to a third party. Defamatory statements have the potential to tarnish a person's morality or integrity, or even to discredit a person's financial standing in the community. A person found guilty of making a defamatory statement is assessed the monetary value of the harm caused by his or her statement. In addition, the plaintiff in a defamation action has the burden of proving the elements of the tort.

An entity that publishes or distributes a defamatory statement made by another person is also liable. An entity, such as a newspaper, that repeats or otherwise republishes a defamatory statement is subject to publisher liability because the injured party is harmed every time the statement is repeated. However, an entity, such as a bookstore, that only distributes or transmits a defamatory statement, is subject to distributor liability only if the entity knew or should have known that the statement was defamatory. A distributor should know' that a statement is defamatory if a person of reasonable prudence and intelligence or of the superior intelligence of the distributor would ascertain the nature of the statement.

One could claim immunity from the liability if one successfully proves that the statements were published as facts, not opinions or ideas. For example, writing, I think that someone is accepting bribes.' is not libel because it is published as an idea of the publisher. On the other hand, if the publisher writes, this person is accepting bribes.' and the statement is proved to be false, then the publisher can be considered guilty of libel. However, the I think' or I believe' clause is not always a valid exemption from libel law, if the implication is that the author is indeed attempting to convey factual information.

The issue of whether an allegedly defamatory statement is one of opinion or fact is one of the more difficult and common questions in a defamation suit. Courts have held that merely prefacing an otherwise defamatory statement with the words I believe'' is not enough to eliminate the implication that the statement was intended to communicate facts.

The plaintiff must prove that some form of damage occurred from the published statement. The damage may have been tangible losses, such as the loss of a job, financial loss, or the damage may have been intangible such as the loss of reputation and respect in a community.

No claim of defamation would arise if it's a fair, true and impartial account of:

1. A judicial proceeding, unless the court has forbidden the publication
2. An official proceeding, to administer the law.
3. An executive or legislative proceeding
4. The proceedings of a public meeting with a public purpose
5. Reasonable and fair comment on or criticism of an official act of a public official or other matter of public concern published for general information.

Public figures such as politicians have less protection under libel law than average individuals. They cannot take action unless they can prove that the statement published about them is of malicious intent and not simply of misinformation. The reasoning behind this is that in theory a public figure can restore his or her reputation more quickly and easily expressly because he or she is already in the public eye and commands the attention of that public.

With the explosive growth of the Internet as a medium used to share information quickly and inexpensively between people, we are faced with the problem of a large decentralized global forum with very little regulation. What happens when a law is broken, and one must place accountability? How does one enforce legislation that may conflict with other codes from other communities to which the Internet extends?

Many questions arise from the issues revolving around the Internet and libel laws. What court precedents have there been in regards to cyber libel? What issues did they

Notes

address? And how those cases laid down the grounds for future legislation? As of late, there have been a few major cases that have strongly affected the courts decisions in case law. However, due to the constant changing nature of technology and the needs that come about from differing use of that newly developed technology, amending case laws is nearly inevitable. Yet, we must drive the formation of the new laws, which are to regulate or not to regulate the Internet, to take into consideration the possible effects and the needs of the future developments in cyberspace.

3.4 Defamation and Liabilities of ISPs

Internet defamation law is complicated by the tricky question of liability of system operators. In defamation law for print and broadcast media, liability is sometimes considered to extend beyond the defamer himself, for instance, the writer of a libelous newspaper column, to the publisher of the material. The idea of holding publishers responsible for libelous material in traditional media has been thoroughly tested and defined in court; there are clear precedents for determining who is liable for defamatory statements in these media. On the Internet, however, such issues are considerably more nebulous.

A sysop, or system operator, is defined as a person or organization who in some way manages the publication/distribution of material online. The most common example is the operator of a bulletin board where users are permitted to post messages which can then be read by other users. Such bulletin boards may be exclusive to a limited group of subscribers, or they may be accessible to anyone on the Internet. The exact role of the sysop can range from merely providing technical support for the posting and reading of messages to carefully reading and editing all published submissions. It is this disparity in the functions of individual sysops that leads to questions about the extent of a sysop's liability in individual cases.

One view of a sysop is as a common carrier, much the way telephone companies are legally viewed. Just as telephone companies attempt no control over what information is communicated across their wires, and are not held legally liable for the content of such communication, this view of a sysop indicates that the sysop provides a forum for any message the user wishes to communicate and is therefore not liable for the content of such a message. For such a definition to apply, the sysop would have to take no editorial or censorial control whatsoever over any postings; only then can he be considered a common carrier. An example of this might be the host of a live-chat room who in no way limits access to this chat room or monitors the conversations which take place therein.

The opposite role from a common carrier is what is called a publisher; in the case of print media, this is the company that actually prints the newspapers containing defamatory

material. A publisher is held legally liable for the information it prints because it exercises full editorial control over that information; it is therefore assumed to be in a position to monitor its content for defamatory material. Many sysops are deemed to fit this role much more closely than that of distributor or common carrier, as past court decisions on sysop liability have shown. In Stratton vs. Prodigy a judge noted that Prodigy did exercise control over its content and could therefore be held responsible for that content. This definition of Prodigy as a publisher was later changed, but some sysops are still considered publishers under the law. A more definitive example would be a newsgroup moderator who reads and edits all material before any is posted; this moderator then clearly takes an active role in the dissemination of defamatory information.

A third category, between common carrier and publisher, is the category of distributor. Again, an analogy to print media is useful; the distributor in this case would be the newsstand which may sell a newspaper containing defamatory content. The newsstand is not assumed to be aware of the content of all the publications it sells and is therefore not held responsible for that content. However, in some situations, the newsstand may in fact be aware of defamatory content; in this instance, it can then be held liable for continuing to distribute this content. In general, a distributor is seen as taking only a passive role in possible defamation and is therefore not liable; only when some deliberate transgression such as failing to remove material it knows to be defamatory can be proven is the distributor liable. This category, sitting in the middle ground between two extremes, is the most difficult to define and deal with, but it seems to be the appropriate designation for many system operators, who will in general not attempt to monitor content but may take action to remove objectionable content if it is brought to their attention.

In Cubby vs. CompuServe, CompuServe was deemed a distributor and therefore not held liable for defamatory material of which it could not be expected to have knowledge. However, the categorization also implies that if CompuServe had been made aware of this material, it would have been obligated to remove it. Finally, the case of Zeran vs. America Online, in which a user was victim of a malicious hoax. The courts ruled in favor of America Online, upholding that interactive computer service providers may not be held liable for posting defamatory statements posted by 3rd parties via the ISP. Effectively, this decision reversed the findings of Stratton Oakmont, Inc. vs. Prodigy.

3.5 Problems in applying traditional methods

Although these definitions can be and have been applied to system operators in Internet defamation cases, some problems do arise with such categorization. For instance, when

Notes

Prodigy was deemed in court to be a publisher, many were concerned that penalizing a service for attempting to maintain control of its bulletin boards could discourage any attempts at control whatsoever. Not only could this conceivably make it easier for defamers to spread on-line, it also makes it more difficult for a service to forbid flaming or, like Prodigy, provide a family- friendly forum for communication, or even to focus that forum on discussion of a specific topic, as many bulletin boards do. Further, laws that hold system operators

liable for their content can, by making the system operator's position a hazardous one, discourage people and organizations from taking on this role, therefore reducing the usefulness of the Internet as a forum for communication among all users. There are some who will argue that this ultimately results in an unnecessary restriction on free communication, and that system operators should therefore not be held liable for defamation or other violations on their services under any circumstances. Others, of course, argue that defamation is a serious enough problem, especially on a forum like the Internet where false information is so easily spread, that all possible efforts should be made to discourage it, and this extends to making sysops responsible for the material they make available. The issue is new enough that neither courts nor legislation have yet rendered definitive verdicts on these questions; only time will tell how they are ultimately answered.

Recently, a leading Indian property developer in India launched a mega housing project. The developer advertised on the internet and attracted buyers online as the company planned to sell more than 50% of their property to overseas buyers. When potential customers started searching the site to know more about the projects, they were directed to blog sites, which spoke of the problems in their existing projects, and included images and videos. Subsequently their competitors used these blogs to advertise their own properties.

An investigation found that these blogs were hosted on servers based abroad and it was difficult for a local Indian company to go against them. Cases were filed in the US and Germany using privacy laws, which resulted in removal of the blogs. But the damage had already been done.

3.6 Literature Review

A. The United States

Currently libelous messages placed on the Internet are treated the same as libelous messages published in any other medium. However, because the author can easily keep

his or her identity a secret, there is frequently a problem in finding a responsible party. Recent cases indicate that owners and operators of online service providers may be liable for what is placed on their servers. Whether or not the Internet service provider is responsible depends on whether the courts consider the Internet service provider to be a publisher or a distributor. Distributors and publishers are treated differently under traditional libel law.

- Distributors such as newsstands, bookstores and libraries are usually not liable for anything that they sell.
- Publishers, such as newspapers and publishing houses are held responsible for materials that they print.

On the Internet, if the service provider is found to be a distributor, the Internet service provider will not be considered liable for materials that appear on its servers. If, however, the Internet service provider is considered to be a publisher, then it will be held responsible for everything that appears on its servers.

B. Great Britain

Material published on the web falls under the same libel laws as material published in any other medium. The British libel law differs from American libel laws in approach. British libel laws are considered pro-plaintiff, meaning that the defendant must prove that she or he did not commit libel. This is the opposite of American libel law, which places the burden of proof upon the plaintiff to show that the alleged libelous statement contained malice and caused damage.

The Defamation Act of 1996 holds Internet service providers responsible for what they publish under British libel laws, albeit in only a very limited scope. This act does not hold Internet service providers responsible if they are not primarily responsible for material in question.

The Defamation Act is looked upon by British lawmakers as a way of limiting potential libel lawsuits. The act will make libel cases cheaper and more quickly resolvable:

- The act will allow judges to suggest money damages and offer Internet Service providers the option of apologizing to the plaintiff and paying him or her money damages.
- Defendants will also be able to offer amends under the defense of innocent dissemination.
- Defendants will be able to reduce their damages if they can prove that the plaintiff has a general bad reputation.

Notes

C. Singapore

Singapore has extremely strict libel laws compared to the American system. Singapore leaders have firmly stated that libel on the Internet will not be tolerated and abusers will be severely punished. On March 6, 1996, Internet service providers became responsible for anything that they print. Further, all Internet service providers must register with the Singapore Broadcasting Authority. The Singapore government has developed a national phone line system through which individuals can access the Internet. The phone lines can be monitored and abusers can then be found.

This law can be ineffective for two reasons:

1. The accessibility of foreign phone lines- Individuals can easily dial into a foreign phone system to access the Internet and bypass the monitoring system in Singapore.
2. The existence of cybercafés- Cyber cafes is popular locations where young people gather. The young people socialize and also surf the Internet. The computer user pays a fee for the Internet time and, to the frustration of the Singapore government, can thereby send anonymous messages.

The Singapore government is also advancing an educational program on Internet etiquette and hopes to teach students how to use the Internet responsibly.

D. Canada

In Canada, there have not been any landmark cases that would determine the policy with which the Canadian government will treat Cyber libel. The existing libel codes hold that the defendant using a defense of innocent dissemination will succeed if the defendant demonstrates:

1. The defendant does not know of the libel contained in the work authored or published by him or her.
2. There was no reason for the defendant to suppose that the work he or she authored or published would be libelous.
3. It was not negligence on the defendant's parts that he or she did not know that the work contained libelous material.

E. India

The Indian Penal Code, 1860 defines defamation as statement or words which are published and calculated to expose any person to ridicule, contempt or hatred or which aim to injure the said person in his vocation, business, trade, profession or office, or which aim to cause him to be shunned or avoided in public and in society.

The important word here is ―published which implies that, for a statement to be considered defamatory, it should be communicated to someone other than the person to whom it is addressed.

Though the Information Technology Act, 2000 does not specifically define defamation as an offence, it is clear that the definition of publishing' is wide enough to include statements made on the Internet. The medium of publication is immaterial in cases involving defamation because, just as in the real world, everyone online has the right to reputation.

Online defamation is, in fact, the most dangerous because of the relatively low cost of setting up a site, the ability to disguise identities and ease with which uncensored information can reach with a limitless audience.

You can have a defamatory statement spread via a site, text message, email or discussion board, and get sued for it, too. Worse, you are guilty even if you have simply ―or even wrongly―forwarded a defamatory email, since every subsequent publication' is a fresh offence. Similarly, owners, administrators and coordinators of any such site will also become a party to the suit.

What about the Internet Service Providers (ISPs) that host these pages? Can they also be held liable? Section 501 of the IPC states that whoever prints any matter, knowing or having good reason to believe that such matter is defamatory, would be liable to imprisonment of two years, or fine, or both.' This has been the bane of many publishers, who have been held liable for defamatory matter printed in their newspapers.

The IT Act, however, clarifies that though the ISPs would ordinarily be liable for the abuse of services provided by them, they may be excused if it is proved that the offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent it.' This is in keeping with global trends which hold that while ISPs should be encouraged to develop some kind of supervisory mechanism, due regard must also be given to the physical difficulties of censoring each and every statement on the Internet.

There arises difficulties of jurisdiction and lack of legal awareness amongst Net users in the country. Most defamatory sites and mailing lists are cunningly uploaded from other countries, outside the jurisdiction of our courts, making punishment by Indian authorities a pipe dream.

3.7 Laws Applicable in India in cases of Cyber Defamation

In India Cyber Defamation results in Civil as well as Criminal proceedings against the accused. Some the Acts and rules that deals with Cyber Defamation are The Indian Penal

Notes

Code, 1960, The Information Technology Act, 2000, The Code of Criminal Procedure, 1973 and The Indian Evidence Act, 1872. The Charging Act for prevention of Cyber Crimes in India is the Information Technology Act, 2000. Section 66A of the Information Technology Act, 2000 provides punishment for Online Defamation. Section 66A can be read as follows:

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

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

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

(b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes 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 purposes of this section, terms “Electronic mail” and "Electronic Mail Message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

Section 65A and Section 65B of The Indian Evidence Act, 1872 provides for Admissibility of electronic records as evidence. Some of the sections of Indian Penal Code, 1960 that deal with Cyber defamation are Section 499, 500 and 503.

3.8 Different Legal Approaches to Cyber Libe

Because the Internet is a global medium and every nation treats libel differently, the plaintiff now has the option of selecting the most favorable forum in which to sue. Since the Internet is accessible from virtually anywhere on the globe, the plaintiff has many forums to choose from. This causes potentially serious problems for Internet service providers. Specifically, the Internet service provider might publish some material in a place where they would not be held liable in a defamation complaint, but be sued in a place where they will be responsible for anything that they put on the Internet.

3.9 Judicial Pronouncements W.R.T. Cyber Defamation in Corporate World

Notes

SMC Pneumatics (Indi(a) Pvt. Ltd. v. Jogesh Kwatra

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature.

Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employee could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an exparte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

In case of Tata Sons Limited vs Greenpeace International & Anr3, the Hon'ble High Court of Delhi Made the Following Observations:

“It is true that in the modern era defamatory material may be communicated broadly and rapidly via other media as well. The international distribution of newspapers,

Notes

syndicated wire services, facsimile transmissions, radio and satellite television broadcasting are but some examples. Nevertheless, Internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by the features described above, especially its interactive nature, its potential for being taken at face value, and its absolute and immediate worldwide ubiquity and accessibility. The mode and extent of publication is therefore a particularly significant consideration in assessing damages in Internet defamation cases."

3.10 Misuse of Cyber World in Terms of Defamation

Unfortunately, the ease of use of these online media has on several occasions been misused by unscrupulous individuals for publishing defamatory remarks in the cyber world. At present, reported cases of cyber defamation have been on the rise. In relation thereof, it is necessary to examine the efficacy of the existing regulatory regime that governs such a crime.

3.11 Protection in Cyberspace

Privacy as a human right may be a novel concept to some; however, it is actually enshrined in the United Nations Universal Declaration of Human Rights. Moreover, digital privacy is emerging as an important human right particularly because it may be subjugated so easily. The Global Network Initiative states rivacy is a human right and guarantor of human dignity'. important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.' Unfortunately, legislative priorities largely appear to exclude digital privacy. According to the Electronic Frontier Foundation, ' the law has yet to catch up to our evolving expectations of and need for privacy.' We see this in the U.S. where legislators have yet to update the Electronic Communications Privacy Act of 1986. At the same time, some question the motives of government action (or inaction) and express concern over what they perceive as an overstepping of authority, particularly regarding the collection, retention and analysis of personal data. In Germany, for instance, the Supreme Courtruled that country's data retention law unconstitutional last year.

While the future state of regulation regarding digital privacy may be uncertain, many global companies are seeking to assure alignment between their human rights policies and practices and the United Nations Guiding Principles on Business and Human Rights: the "Protect, Respect and Remedy" Framework launched formally in April 2011. While the framework recognizes the State obligation to protect human rights, it also recognizes a corporate responsibility to respect human rights, act with due diligence, and address

adverse impacts.' Leadership companies, such as those in high tech, have been notably proactive in their efforts to address human rights. This is particularly true of Symantec who is intimately familiar with the intersection of digital privacy and security through its core business:

"The protection of individual privacy afforded by our products is critical to the protection of human rights. Indeed, many of our products, including encryption, endpoint protection, online backup, and antivirus software support the first three UNGC principles by enabling individuals to protect the secrecy of their communications and work products, to store their information with a trusted vendor, and to monitor and track attempts of intrusion into their information from other individuals and/or governments."

3.12 Human Rights in Cyber Space

To mention but a few fundamental freedoms and privacy human rights that are dealt with in this context are, for example, free expression of belief, political opinion, art and written texts; the free and equal access to information; and the protection of privacy issues such as family relations, friendships or health issues. Furthermore, human rights in cyberspace is about the protection and security to be free from harassment and persecution on internet for a based on one's own political, ethical or gender identity as well for hers or his private professional, educational or health data without his or her consent. It is about protecting one's own intellectual property and creativity, i.e. art, movies, pictures, literature, scientific results, as well as having access at any time to fair and open trials – to name but a few.

The often proclaimed Right to Internet' which aims to allow individuals have access to internet at any time and the Right to be Forgotten' which assures that one's own private data remains private and can be deleted at any time, are already part of the overall human rights standards concerning access to information, the right to privacy and data protection (as in the EU Fundamental Rights Chart(a) and participation. Yet, how to realize these rights and turn them into active legislation has to be seen. Case law will most likely take quite some time to establish interpretations of these rights, although the Research Division of the European Court of Human Rights has already in 2011 published a groundbreaking documents on the potential the Case-law concerning data protection and retention issues relevant for the internet could mean in future decisions taken by the court. In this document the freedom of expression, intellectual property and issues of cybercrime are seen the major deficits that yet have to be further defined and interpreted through case law.

Notes

It is therefore no longer an issue of international debates whether freedom rights exist or not, but rather how to implement and enforce them into national legislation. During the conference, all UN member states confirmed that all human rights derive from the dignity and worth inherent in the human person, and that the human person is the central subject of human rights and fundamental freedoms, and consequently should be the principal beneficiary and should participate actively in the realization of these rights and freedoms.

3.13 Adopting Cyber Security Strategies that Violate Human Rights

The use of loaded, imprecise language has, indeed, had far-reaching consequences, as many governments are using vague internal and external threats as arguments to justify ever greater investments in cyber arms and mass surveillance schemes, and ever greater governmental control of the Internet and their citizens. The sense of alarm embedded in cyber security narratives has clouded the need to objectively and evidentially substantiate the likelihood and nature of the dangers at hand.

It has also given rise to the impression that all responses are appropriate and legitimate. For example, as we pointed out earlier, in many countries, both democratic and nondemocratic, the threats posed to national security have long been used to justify extensive surveillance mechanisms, with more and more citizen data collected and easily accessed by state authorities. Other ominous

security' measures include developing so-called Internet kill switches' (the notion of shutting down the Internet in order to protect it), restricting the use of encryption, implementing filtering and blocking mechanisms and introducing real name policies. Such measures often pose threats to civil liberties, yet they tend to lack judicial oversight as well as public data on which to judge their effectiveness (often because of claims that disclosure would impact on security efforts). While it is not at all clear that they improve security, they frequently risk erasing the benefits the Internet brings.

3.14 Constitutional Mandates

There is an inherent and natural conflict between right to privacy on the one hand and the right to information and right to know on the other. A law pertaining to data protection should primarily reconcile these conflicting interests. Thus, the data of individuals and organisations should be protected in such manner that their privacy rights are not compromised. At the same time the right to information U/A 19(1)(a) and the right to

know U/A 21A law relating to data protection should be in conformity with the following mandates, as imposed by the sacred and inviolable Constitution of India:

Right to privacy U/A 21: The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate. The term ―privacy denotes the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others. It means his right to withdraw or to participate as he thinks fit.

It also means the individual's right to control dissemination of information about him as it is his own personal possession. Privacy primarily concerns the individual. It, therefore, relates to and overlaps with the concept of liberty. The most serious advocates of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other rights and values. The right to privacy as an independent and distinctive concept originated in the field of Tort law, under which a new cause of action for damages resulting from unlawful invasion of privacy was recognized. This right has two aspects which are but two faces of the same coin: (1) the general law of privacy which affords a tort action for damages resulting from an unlawful invasion of privacy, and (2) the constitutional recognition given to the right to privacy which protects personal privacy against unlawful governmental invasion. The first aspect of this right must be said to have been violated where, for example, a person's name or likeness is used, without his consent for advertising or non- advertising purposes or for that matter, his life story is written whether laudatory or otherwise and published without his consent. In recent times, however, this right has acquired a constitutional status. India is a signatory to the International Covenant on Civil and Political Rights, 1966. Article17 thereof provides for the―right of privacy. Article12 of the Universal Declaration of Human Rights, 1948 is almost in similar terms. Article 17 of the International Covenant does not go contrary to any part of our municipal law. Article21 of the Constitution has, therefore, to be interpreted in conformity with the international law.

3.15 Information Technology and the Law of Privacy

Advances in computer technology and telecommunications have dramatically increased the amount of information that can be stored, retrieved, accessed and collectedalmost instantaneously. In the Internet age, information is so centralized and so easily accessible that one tap on a button could throw up startling amounts of information about an individual. In terms of electronic information, a person should be able to keep personal affairs to himself. Advances in computer technology are making it easy to do what was

Notes

impossible not long ago. Information in many databases can be cross-matched to create profiles of individuals and to even predict their behavior. This behavior is determined by individual's transactions with various educational, financial, governmental, professional and judicial institutions. Major uses of this information include direct marketing and credit check services for potential borrowers or renters. To the individual, the result of all this information sharing is most commonly seen as increased —junk mail.

There are much more serious privacy issues to be considered. For instance:

4. Every time you log onto the internet you leave behind an electronic trail. Web sites and advertising companies are able to track users as they travel on the Internet to assess their personal preferences, habits and lifestyles. This information is used for direct marketing campaigns that target the individual customer. Every time you use your credit card, you leave behind a trail of where you shopped and when, what you bought, your brand preferences, your favorite restaurant.
5. Employee's privacy is under siege as employers routinely use software to access their employee's e-mail and every move of the employee. Field sales representatives have their movements tracked by the use of location- based tracking systems in new wireless phones.

Thus, the law of privacy has not kept pace with the technological development. It must be noted that the right to freedom of speech and expression and right to privacy are two sides of the same coin. One person's right to know and be informed may violate another's right to be let alone. These rights must be harmoniously construed so that they are properly promoted with the minimum of such implied and necessary restrictions. The law of privacy endeavors to balance these competing freedoms.

Freedom of information U/A 19(1) (a): The right to impart and receive information is a species of the right to freedom of speech and expression. A citizen has a Fundamental Right to use the best means of imparting and receiving information. The State is not only under an obligation to respect the Fundamental Rights of the citizens, but also equally under an obligation to ensure conditions under which the Right can be meaningfully and effectively be enjoyed by one and all. Freedom of speech and expression is basic to and indivisible from a democratic polity. The world has moved towards universalization of right to freedom of expression. In this context reference may be made to Article 10 of the European Convention on Human Rights. Article 10 of the Convention provides that everyone has a right to freedom of expression and this right shall include freedom to hold opinions and to receive information and ideas without interference by the public authorities and regardless of the frontiers.

Again, Article 19(1) and 19(2) of the International Covenant on Civil and Political Rights declares that everyone shall have the right to hold opinions without interference, and everyone shall have the right to freedom of expression, and this right shall include freedom to seek, receive and impart information of ideas of all kinds regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice. Similarly, Article 19 of Universal Declaration of Human Rights, 1948 provides that everyone has the right to freedom of opinion and expression and this right includes freedom to hold opini on without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. In the Indian context, Article 19(1) (a) of the constitution guarantees to all citizens freedom of speech and expression. At the same time, Article 19(2) permits the State to make any law in so far as such law imposes reasonable restrictions on the exercise of the rights conferred by Article 19(1) (a) of the constitution in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency, morality, contempt of court, defamation and incitement of offence. Thus, a citizen has a right to receive information and that right is derived from the concept of freedom of speech and expression comprised in Article 19(1) (a). It must, however, be noted that freedoms under Article 19, including

Article 19(1) (a), are available only to citizens of India. An alien or foreigner has no rights under this Article because he is not a citizen of India. Thus to confer protection upon non-citizens one has to depend upon and apply Article 21 which is available to all persons, whether citizen or non-citizen.

Right to know under Article 21: Article 21 enshrines right to life and personal liberty. The expressions right to life and personal liberty' are compendious terms, which include within themselves variety of rights and attributes. Some of them are also found in Article 19 and thus have two sources at the same time.

In R.P. Limited v Indian Express Newspapers the Supreme Court read into Article 21 the right to know. The Supreme Court held that right to know is a necessary ingredient of participatory democracy. In view of transnational developments when distances are shrinking, international communities are coming together for cooperation in various spheres and they are moving towards global perspective in various fields including Human Rights, the expression liberty' must receive an expanded meaning. The expression cannot be limited to mere absence of bodily restraint. It is wide enough to expand to full range of rights including right to hold a particular opinion and right to sustain and nurture that opinion. For sustaining and nurturing that opinion it becomes necessary to receive information. Article 21 confers on all persons a right to know which include

Notes

a right to receive information. The ambit and scope of Article 21 is much wider as compared to Article 19(1) (a). Thus, the courts are required to expand its scope by way of judicial activism. In P.U.C.L v U.O.I the Supreme Court observed that Fundamental Rights themselves have no fixed contents, most of them are empty vessels into which each generation must pour its contents in the light of its experience. The attempt of the court should be to expand the reach and ambit of the Fundamental Rights by process of judicial interpretation. There cannot be any distinction between the Fundamental Rights mentioned in Chapter-III of the constitution and the declaration of such rights on the basis of the judgments rendered by the Supreme Court. Further, it is well settled that while interpreting the constitutional provisions dealing with Fundamental Rights the courts must not forget the principles embodied in the international conventions and instruments and as far as possible the courts must give effect to the principles contained in those instruments. The courts are under an obligation to give due regard to the international conventions and norms while construing the domestic laws, more so when there is no inconsistency or conflict between them and the domestic law.

3.16 Statutory Perspective

The inherent and natural conflict between right to know and right to privacy is also permeating various statutory laws enacted from time to time. These laws, with their conflicting contours, are:

Right to information in cases of venereal or infectious diseases: The welfare of the society is the primary duty of every civilized State. Sections 269 to 271 of the Indian Penal Code, 1860 make an act, which is likely to spread infection, punishable by considering it as an offence. These sections are framed in order to prevent people from doing acts, which are likely to spread infectious diseases. Thus a person suffering from an infectious disease is under an obligation to disclose the same to the other person and if he fails to do so he will be liable to be prosecuted under these sections. As a corollary, the other person has a right to know about such infectious disease. In Mr. X v Hospital Z the Supreme Court held that it was open to the hospital authorities or the doctor concerned to reveal such information to the persons related to the girl whom he intended to marry and she had a right to know about the HIV Positive status of the appellant. A question may, however, be raised that if the person suffering from HIV Positive marries with a willing partner after disclosing the factum of disease to that partner, will he still commit an offence within the meaning of Section 269 and 270 of I.P.C. It is submitted that there should be no bar for such a marriage if the healthy spouse consents to marry despite of being aware of the fact that the other spouse is suffering from the said disease.

The courts should not interfere with the choice of two consenting adults who are willing to marry each other with full knowledge about the disease. It must be noted that in Mr. X v Hospital Z (II) a three judge bench of the Supreme Court held that once the division bench of the Supreme Court held that the disclosure of HIV Positive status was justified as the girl has a right to know, there was no need for this court to go further and declare in general as to what rights and obligations arise in such context as to right to privacy or whether such persons are entitled to marry or not or in the event such persons marry they would commit an offence under the law or whether such right is suspended during the period of illness. Therefore, all those observations made by the court in the aforesaid matter were unnecessary. Thus, the court held that the observations made by this court, except to the extent of holding that the appellant's right was not affected in any manner by revealing his HIV Positive status to the relatives of his fiancée, are uncalled for. It seems that the court has realized the untenably of the earlier observations and the practical difficulties, which may arise after the disclosure of HIV status.

3.17 Misuse of Privacy and Human Rights

The Information Technology Act, 2000 provides for two measures, in case of wrongful disclosure and misuse of personal data, i.e. civil consequence of payment of compensation and criminal consequence of punishment for commission of offence. Under Section 43A of the IT Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected.

3.18 Summary

Cyber defamation is a growing tool in brand wars in the business world. Government agencies, celebrities and politicians too use these services. It is an organized racket and anyone can hire these racketeers for a price. "Cyber defamation attacks and their counter defences assume paramount importance in today's fragile economic age," says Satheesh G Nair, MD (Apa(c) of Stickman Consulting, a cybercrime investigation firm. He says that in a country that is as socio-culturally varied as India, even the integrity of the nation can suffer on account of cyber defamation. "The ban on bulk SMSs and check on networking sites prior to the recent Ayodhya verdict is a current demonstration of how cyber defamation is of paramount importance," he says.

There is growing awareness among corporates about this trend. Nair says it is hard to take preventive measures. However, some remedial measures can be taken. For example, the company can find out about attempts to defame it before others take note

of it. "Be informed about what competitors/customers/enemies are talking about you before someone else tells you," Nair says. Cyber detectives can help in this.

Notes

Communication is an art that has developed immensely over the past few centuries and an art that will continue to reinvent itself to unimaginable technological advance. Starting with the advent of the printing press in the nineteenth century, to the era of the Internet that we are living in today, communication has become astoundingly simple and continues to become simpler by the day.

The Law however, developed though it may be in the United States and Europe, is not growing at the same rate as the Internet is, in India. There are court cases in progress right now that will decide if access providers such as Prodigy, America Online and CompuServe are responsible for defamatory remarks broadcast over their services, but there is no legal ambiguity about whether individual users can be sued for making defamatory or libelous statements. Individual users are responsible for making sure the information they distribute is not libelous or defamatory.

The Internet has made worldwide, instantaneous communication easy. The average user now has the power to be heard by hundreds or even thousands of other users, but in terms of libel and defamation, the Net is not a new world of freedom. The reality is that libel and defamation laws are enforceable in the virtual world just like they are in the real world.

Cyber Defamation in Corporate world can have far reaching effects on the organizations in some cases. However there are laws in place to deal with cyber defamation and with admissibility of electronic records as evidence things have been eased. If the plaintiff is able to prove that defamation has occurred then the onus lies on the defendant to prove that he was innocent. Further there are also Cyber Crime Investigation Cells to deal with Cyber Crimes in India.

Organizations and endeavors, instruction and preparing, accounts and money matters, private correspondence, and even wellbeing and personal issues are presently by offering private information; billions of internet users have officially made virtual twins in this new space, while never having an opportunity to erase information. Organizations and undertakings, training and preparing, funds and mass trading, private correspondence, and even wellbeing and personal issues are presently managed by any individual who looks for access to it in this "unending" space.

3.19 Review Questions

1. What do you understand by online defamation?
2. Discuss the liabilities of ISPs in the matter of cyber defamation.

3. Discuss some problems which occur in applying traditional methods.
4. What do you mean by cyber libel?
5. Discuss few judicial pronouncements which relate cyber defamation of corporate world.
6. How would you protect your privacy in virtual world?
7. Discuss, how cyber security strategies violates human rights?
8. Explain some constitutional mandates which relates to privacy and human rights?
9. Explain the difference between privacy and human rights?
10. How IT Act, 2000 involve itself in the law of privacy?

3.20 Further Readings

- A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime
- Introduction to Indian Cyber Law by Rohas Nagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf
- Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
- Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
- Cyber Forensics in India; retrieved from http://perry4law.org/cfii/
- Digital Evidence & the Indian Law by Asian School of Cyber Laws; retrieved from http://www.asianlaws.org/del.pdf

UNIT–4

Notes

Dispute Resolution in Cyberspace

(Structure)

4.1 Learning Objectives

After studying the chapter, students will be able to:

- Discuss the Online Dispute Resolution;
- Explain the nature of Online Dispute Resolution;
- Discuss the beneficial in disputes resolutions;
- Explain the Law Enforcement Agencies for cyber space;
- Discuss the Scope and Development of Cyber Laws;
- Explain the Law Enforcement Agencies are done;

- Discuss the Conventions on Cyber Crime Treaty;
- Explain the UN and US policy;
- Discuss the different treatise are dealing with Cyber crimes;
- Describe the misuse of these International Treatise are done.

Notes

4.2 Introduction

Online dispute resolution (ODR) is a branch of dispute resolution which uses technology to facilitate the resolution of disputes between parties. It primarily involves negotiation, mediation or arbitration, or a combination of all three. In this respect it is often seen as being the online equivalent of alternative dispute resolution (ADR). However, ODR can also augment these traditional means of resolving disputes by applying innovative techniques and online technologies to the process.

ODR is a wide field, which may be applied to a range of disputes; from interpersonal disputes including consumer to consumer disputes (C2C) or marital separation; to court disputes and interstate conflicts. It is believed that efficient mechanisms to resolve online disputes will impact in the development of e- commerce. While the application of ODR is not limited to disputes arising out of business to consumer (B2C) online transactions, it seems to be particularly apt for these disputes, since it is logical to use the same medium (the internet) for the resolution of e-commerce disputes when parties are frequently located far from one another.

ODR is a highly recommended method because it is not as time consuming as normal litigation, disputes are easily documented and the person need not submit to the jurisdiction of any court. There are three main models of online dispute settlement:

1. **Cyber settle:** wherein there is automated negotiation mechanism
2. **Online mediation:** wherein there is live mediation
3. **Online adjudication:** wherein there is online arbitration

According to her, the Arbitration and Conciliation Act, 1996, and the Information Act, 2000, are well equipped to cater to the online system of dispute resolution. The steps that need to be taken are:

1. Create more awareness
2. Draft rules in case of any ambiguity
3. Extend the system by promoting it in all legislations
4. Parties should be made to sign a binding agreement before they enter into the online dispute resolution system.

Online dispute resolution is simple, speedy and provides an easy and expeditious way of resolving problems for parties which are in different parts of the world.

Notes

Delhi High Court has e-courts but they are not as functional as they ought to be. But once they are utilized properly, it will be possible to have a successful arbitration system. The Supreme Court has already decided upon this issue and held that choosing an umpire online is valid. According to Hon'ble Justice Sen., paper filing etc. should have already been done away with since e- filing is the order of the day.

Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe.

Until recently, many information technology (IT) professionals lacked awareness of an interest in the cybercrime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases.

Finally, there was a certain amount of antipathy—or at the least, distrust— between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet close cooperation between the two is crucial if we are to control the cybercrime problem and make the Internet a safe place' for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cybercriminal.

IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offense. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes into organized categories.

Today most cybercrimes such as 419 Nigerian attacks or fake employment or lottery scams are trans-border. In the age of social media and cloud computing, investigation of cybercrimes requires data and evidence often located in another jurisdiction. There are widespread phishing attacks, global attacks on infrastructure, transnational organized crimes and cyber wars. Therefore, international cooperation in cybercrime matters is not an advantage but a necessity today.

The Information Technology Act, 2000 also applies to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves as computer, computer system or network located in India. However, in-case there is an offence committed by any foreign national under IT Act, 2000 such as identity theft (section 66C of IT Act, 2000 and/ or hacking under Section 66), legal assistance and cooperation will be required from concerned Authorities in the foreign country where the foreign national resides for any investigation / prosecution/ extradition.

This is difficult to obtain in the absence of a Cybercrime Convention that India is signatory to (as India has not signed any) and/or a Mutual Legal Assistance Treaty (MLAT) for cooperation on cybercrime matters (as India has not signed any).

Although India has signed MLAT with few countries for legal assistance on criminal matters, a crime/ cybercrime may not be covered by it in those arrangements which require dual criminality to be satisfied and one of countries does not consider a cybercrime to be a crime as per its laws. Moreover, the scope of assistance agreed in a MLAT India has signed with other countries on criminal matters is not adequate to effectively handle cybercrime matters, particularly because digital medium is dynamic.

A cybercrime can play havoc in cyberspace if it is a bot attack. As the speed of committing crime and impact thereof is greater in cybercrime cases and because electronic evidence can be easily tampered or is volatile, it is imperative to trace the offender in the shortest possible time and preserve original evidence. Moreover, tracing of offender in cybercrime cases may be more difficult due to availability of several techniques to camouflage one's identity using steganography, onion routing or other hide IP practices.

In the MLATs signed by India for criminal matters, in general, there are no time limits for execution of requests and therefore such MLATs may not provide efficient procedure or cooperation framework in cybercrime matters. Effective investigation and prosecution of cybercrime matters requires quick action as evidence is volatile and failure to collect electronic evidence in a timely manner can stifle effective investigation.

India is currently a signatory to UN Convention against Transnational Organized Crime. This Convention applies to criminal matters in general and may not be effectively

Notes

used in cybercrime cases. In 2013, a comprehensive study was conducted by UN on the emerging problem of cybercrime with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. It was found that there is a large diversity of national cybercrime laws on international cooperation and there is need for harmonization of national legal frameworks-definition and scope of cybercrimes, investigative powers, and admissibility of electronic evidence. It was felt that the Convention and national legal frameworks need to be adapted by making suitable amendments to deal with rising cybercrimes.

4.3 Evolution of ODR Industry

Online dispute resolution (ODR) was developed to circumvent clogged and slow moving courts and the hassle of physical dispute resolution mechanisms. ODR tries to harness the power of internet to resolve disputes, by reducing costs, doing away with the necessity to travel to attend courts and generally making the entire process faster and efficient through use of web based technologies. This is the basic precept on which ODR is built. If possible, this could be a significant improvement over the current alternative dispute resolution methods such as traditional arbitration, mediation etc. ODR debuted in 1998 in United States and not much is known about it in India.

4.4 Resolving Business Disputes

For business, time is money. Disputes are like cancer which should be stopped from spreading as soon as possible. The business disputes may be business to business (B2B) or business to customer (B2C). For both type of disputes, litigation is the least favored method of resolution for a variety of reasons – delay being the foremost. ADR methods provide the solution. Methods like negotiation, mediation, conciliation, arbitration and a mix of these have been used and are currently becoming popular for resolution of business disputes. However, the limitation of these methods, particularly, physical presence of both the parties and the arbitrator/conciliator/mediator at one place at a number of meetings, makes even ADR methods quite cumbersome and ineffective There are three current approaches to ODR: cyberspace, non-adjudicative ADR, and arbitration. The first centres on the Internet and information technology. The principle underlying the cyberspace approach is to find better, faster and cheaper ways to resolve disputes with the aid of technology. The non-adjudicative ADR approach to ODR focuses mainly on negotiation and mediation, and how to improve both communications and relationships between parties. The arbitration approach emphasizes rights and applications of law to resolve the dispute with an arbitrator's decision. The impetus behind this approach is the

success of traditional arbitration. If it works so well offline, then it should be adapted online, the reasoning goes.

The major players in ODR are: business community, consumers, and government and ADR institutions. Business community favors ODR because it is private, fast and inexpensive. It also encourages consumer trust. For consumer organisations, ODR enforces consumer rights. Governments see ODR as a tool to provide access to justice that courts are not yet equipped to provide, decrease court congestion and further the e-commerce economy. ADR institutions see ODR as an opportunity to gain the competitive edge. The application of information communication technology (ICT) is evolving as an important means for future resolution of certain types of conflict. ODR will become an increasingly important component of the infrastructure required if online business and other relationships are to realize their full potential.

Globally, the use of ODR is growing and has been well documented over the years and consumer disputes are seen as the main area of growth, together with human resources, government and employment disputes also a fertile ground for this type of technology.

4.5 Why ODR?

Cost and Time

ODR is generally considered a more efficient process than ADR/ litigation because it is quicker and less expensive. Given the fact it does not require physical presence as is the case with ADR and litigation, it saves up on time and cost as may be required.

Modus Operandi

The mode of proceedings in ODR is often decided by the parties unlike court based suits that follow a strict statute determined procedure. Of course, ODR must follow the rules laid down by appropriate legislations and some basic principles that all legal proceedings should follow, but it has the potential to emerge as a more flexible and convenient mode of dispute resolution. Also, ODR is typically less confrontational because it takes place in a much less formal setting on an online platform.

Confidentiality

Confidentiality of matter can be protected far better in an ODR process.

Flexibility

ODR is much more flexible as it is governed by party's agreement or the rules and regulations of the online platform used and is not dependent on the stare decisis (deciding on the basis of precedents) principle just like any other ADR.

4.6 Nature of ODR

Notes

Online and Offline Model of ODR

The potential use of the Internet to resolve international disputes can be divided into two distinct areas: using Internet-related technology to resolve real world' disputes online or partially online and using the Internet to resolve disputes arising on the Internet itself.

For instance, in offline dispute, you can have a clause in your contract with your supplier for resolution of dispute using one of the ODR platforms. As far as online disputes are concerned, the platform you are dealing with might have an inbuilt mechanism as is the case with EBay Procedures adopted for ODR

Online Negotiation

Forums such as Cyber Settle use negotiation for Dispute Resolution. Online negotiation can be of two types, closed model and open model.

Close Model

Online negotiation thrives on technological changes through blind bidding which is one of the most prevalent dispute resolution services available online. The common characteristic of these processes is the parties submission of monetary offers and demands which are not disclosed to their negotiating counterpart, but are compared by computer in rounds. If the offer and demand match, fall within a defined range or overlap the case is settled for the average of the offer and demand, the matching amount, or the demand in the event of an overlap. If the claim is settled, the participants are immediately notified via email

Open Model

Under the open model, a party can view the other's party offer or demand only after having made a demand or offer. Whenever any offer is within twenty per cent of any demand, there is settlement of the median.

Online Mediation

A typical online mediation procedure takes place as follows. The complainant initiates it by completing a confidential form on the provider's website. Then, a mediator contacts the respondent in order for him/her to participate. Both parties set forth the mediation ground rules.

The mediator communicates with the parties, sometimes jointly and sometimes individually, to facilitate an agreement. If an agreement is reached, it usually takes the form of writing.

Thus, the online process does not differ very much from the offline process, except for the expanded use of technology. Email is the mediator's best friend for purposes of framing and moving discussion forward. But email was already used by offline mediators. In online mediation, websites such as Smart Settle, Legal Face Off etc. are providing online mediators with new tools to supplement email with other communication tools including elect ronic conferencing, online chat, video-conferencing, facsimile and telephone.

Online Arbitration

Online arbitration proceeds along different communication stages (process agreement, initial presentations, rebuttals, consideration, and decision). Arbitration is in general a much less complicated communication process than mediation. In the simplest arbitration, software that allows positions to be stated and documents to be shared may provide a sufficient frame for the process.

There are many arbitration service provider in abroad such as American Arbitration Association. AAA is known for handling large, complex cases. In 2011, 46% of the arbitration filed with the AAA involved claims $1,000,000 or more.

4.7 ODR vs litigation

In ODR, cost and time efficiency are typical characteristics as opposed to a judicial process with consumes substantial time and cost for adjudication of disputes. Tyler and Bretherton aptly stated- The difficulty of utilizing traditional dispute resolution methods in low value cross border disputes has led to interest in low cost cases, cross jurisdictional dispute resolution methods'.

ODR denotes greater flexibility as it can be initiated at any point of a judicial proceeding or even before a judicial proceeding begins. ODR can also be terminated if the parties mutually decide that it is not leading to a workable solution. The parties have the autonomy to decide the mode and procedure for online dispute resolution in case disputes arise from a particular e- contract. Even in the absence of a written contract declaring ODR as method of dispute resolution, the parties may adopt ODR methods to resolve their disputes when such disputes arise. Contrary to litigation, the parties are free to choose their governing law of contract, the procedure to resolve disputes, decide on an ODR service provider and provide for other incidental matters. Use of ODR also allows selection of neutral third party from an experienced panel of mediator/ arbitrators which means greater impartiality and parties may present their case on their own without apprehension that their private disputes will flow into the public domain through judicial precedents. The disputes and the negotiations that ensue between parties remains confidential at all times. In B2C transactions, ODR encourages customer loyalty;

in C2C transactions it minimizes acrimony and risk of fraudulent transactions between concerned parties.

Notes

4.8 Benefits

Economically viable: Cost is one of the most crucial factors in dispute resolution, as disputants like to reach an optimal decision at the lowest possible price. ODR best suits the financial demands of all parties to a dispute, as most of the document are exchanged via e-mail and the proceedings take place online as opposed to exchange of documents by post.

The costs related to travel and accommodation, venue for conducting the proceedings is also eliminated. Therefore, carrying out ODR is not only easier and faster, but it is also significantly cheaper

Speedy resolution: One of the main advantages of ODR over conventional ADR is that it is less-time consuming. Where, in ADR it may take several months to resolve a dispute, ODR promises settlement of disputes within a few weeks. Further, the borderless nature of the internet diminishes the communication problems faced by parties and their counsels who may be located in different time zones. Moreover, the internet enables parties to easily obtain data and other information about their cases in real time. In addition to easy accessibility, e -mail simplifies the task of scheduling ODR proceedings and avoids any phone or fax- tags in the process. The internet is also a superior and swifter form of communication, as it facilitates the sending and storing of documents of multiple parties simultaneously, thus saving both time and money.

Non-confrontational mechanism: By removing the physical presence of the adversary, ODR enables the adjudicating body to dispassionately resolve the dispute, purely on basis of the merits of the case. Further, since most of the arguments or dialogues take place asynchronously over the internet, it allows the disputants to reflect on their positions before articulating their response. Additionally, such a mechanism neutralizes any economic or other power disparities that may obtain between the disputants, as there may be several instances where one party to the dispute is a small-time manufacturer/ supplier and the opposite party is global entity.

Neutral forum: The internet offers a neutral forum for adjudication and the home advantage' one of the parties hitherto enjoyed.

Facilitates record keeping: ODR facilitates the process of maintaining the record of the correspondences, pleadings, statements, and other written, oral or visual communications, by relying solely on digital records. This in-turn saves time and money of the parties.

4.9 ODR in India

Online dispute resolution (ODR) in India is in its infancy stage and it is gaining prominence day by day. With the enactment of Information Technology Act, 2000 in India, e-commerce and e-governance have been given a formal and legal recognition in India. Even the traditional arbitration law of India has been reformulated and now India has Arbitration and Conciliation Act, 1996 in place that is satisfying the harmonized standards of UNCITRAL Model. The amendment made in the Code of Civil Procedure, 1908 by introducing section 89 was made to provide methods of alternative dispute resolution (ADR) in India.

ODR in India is facing many legal roadblocks and the same need to be addressed immediately by Indian government. Further, awareness about ODR in India is also missing as per ODR service providers in India.

4.10 ODR in Asia1

Asia is a rich and major continent that has excelled in the utilization of ICTs. Whilst many Asian States merit a mention, this chapter shall focus on China, Japan and India as major ODR players in the Asian continent.

The choice of such three states is not only due to their international standing and weight, but also due to the progressive and accelerated development in the invention and implementation of ICT applications, which certainly impacts the development of ODR schemes.

On such account, the chapter shall be divided into three parts; each part shall be devoted to assess the status quo of ODR in one of the three distinguished states, which have three of the highest Internet and mobile phone usage rates in the world.

For example, China has emerged as one of the largest e-commerce giants with more than 457 million Internet users and 277 million mobile phone Internet users. In Japan, a White Paper entitled Basic IT Strategy‘, released in August 2000 by the Ministry of International Trade and Industry (MITI), has revealed Japan’s ambition to expand its IT infrastructure in support of not only the development of e-commerce, but the eventual implementation of e-Government initiatives.

4.11 Drawbacks

The following drawbacks prevail in the ODR process which hampers its growth as an efficient mechanism for resolving disputes:

Lack of human interaction and miscommunication: The lack of face-to-face interaction deprives the adjudicating authority of the opportunity to evaluate the

credibility of parties and the witnesses. Moreover, the impersonal nature of the internet can potentially cause miscommunication between the parties, which is likely to occur when parties are located in different countries and speak different languages.

Notes

Limited range of disputes: Like ADR, ODR is also best suited to resolve only certain types of disputes, like, e-commerce and domain name disputes. The ODR mechanism may not be suitable for resolving every kind of online dispute, for example, negotiation and mediation may be more suitable in resolving issues such as the damages that may be payable for breach of contract.

Inadequate confidentiality and secrecy of proceedings: The secrecy of proceedings is fundamental to the process of dispute resolution, which ODRs inherits from ADRs. Accordingly, ODR providers have made technological arrangements, such as, installation of various software's, firewalls, etc., to protect the data sent by the parties from data interception, alteration, etc. Though substantial efforts have been made towards creation and implementation of data protection laws, these measures do not ensure 100% protection from hackers and other cyber offenders and require constant updating, despite which there may still exist loop-holes which can be exploited. Thus, inadequate internet security may act as a major deterrent in the growth of ODR.

Inadequate authenticity: Closely related to the issue of security is the issue of authentic identification of the user. In an ADR process, one party can be certain that the other party it is dealing with is the party actually involved in the dispute. However, in cyberspace, it is not easy to verify the authenticity of messages received and it is relatively easy for a third party to impersonate or misrepresent one of the parties in the dispute, causing confusion, thereby defeating the very purpose of adopting ODR.

Jurisdiction: Internet being a borderless medium transcends and challenges traditional concepts of jurisdiction. This leads to problem in deciding the applicable substantive law which is to be applied to the dispute. This issue can only be resolved by parties clearly identifying the applicable substantive and procedural laws in the clause whereby they agree to submit the dispute to resolution by ODR. Ultimately, the resolution of this issue would be contingent upon the pronouncement of the court systems in different jurisdiction which would examine and interpret such ODR clauses, but this process is inescapable and inevitable and cannot be circumvented.

Hindrances at pre-trial stage: A significant component of the pre-trial stage is discovery; interrogatories and collation of evidence in support the respective contentions of the parties. This discovery or fact-finding process may be minimized in the ODR process to speed the process of settlement of dispute. However, in a situation where

the facts are disputed, a limited discovery procedure may serve to limit the fact finding capacity of the adjudicating authority to discover the true and correct state of facts. Further, limiting or eliminating discovery process may offend the due process, causing the courts to strike them down as they do not meet the minimum requirements of due process.

Publication of proceedings and award: If ODR is to be encouraged as a popular mode of dispute resolution, details of proceedings and decisions would be required to be published which ensures transparency. But, this contradicts the very essence of ODR, which is respecting the confidentiality and right to privacy of the parties. Thus, the fate of ODR hangs in balance with one school of thought demanding absolute secrecy of proceedings and the other school seeking publication of proceedings and the decisions. As a matter of practice, currently, all ODR providers keep the proceedings confidential and release information only if both the parties agree to publish the decision.

Difficulty in enforcement of online awards: Like ADRs, in the case of online arbitrations, once the decision has been rendered, the same has to be enforced in the appropriate court. In several jurisdictions, including India, the orders in execution are subject to appeals and this serves to protract the process of execution. Going by this principle, unless the parties are assured of the enforcement and implementation of the decisions, disputants may not have much faith in online proceedings. Further, enforceability of foreign decisions pronounced after completion of ODR proceedings is also an issue which must be considered while agreeing to an ODR clause.

Challenging an award: Since ODR proceedings are conducted online, another issue requiring clarity is the intervention of a court during or after the completion of the proceedings and/or pronouncement of the decision. This will again raise the question of: (a) the enforcement of the decision of the court in the country where the opposite party operates/resides; and (b) appeals against the decision of the court and enforcement of the said decision.

4.12 Future of ODR

As said by Jeffrey N. Rosenthal is an attorney with Blank Rome, the attractiveness of ODR services to the world-at-large will likely only increase. The availability of such systems can build trust in a company by reminding consumers and corporations dealing with it that a neutral third-party can cheaply and easily resolve disputes.

However, India is yet to exploit the benefits of ODR. There is an acute lack of legislative action or awareness in this regard. This problem is teamed up with the lack

Notes

of ODR institutions in India. Given the fact that its being predicted that the SME Sector would be the driving force for growth in India, there is huge scope for application of ODR Mechanism in resolution of dispute for SMEs as ODR can be a cheap and easy way out of a disputes that are bound to arise during the course of business.

Electronic commerce brings both comforts and discomforts to its users. The comforts include on the spot sales and purchase, competitive costs, convenience, saving of time, etc. The discomforts include frauds and cybercrimes committed against e-commerce users. At times there are disagreements and dissatisfactions as well among buyers and purchasers that cannot be resolved using traditional litigation methods.

This is the reason why we need alternative dispute resolution (ADR) mechanism to resolve e-commerce disputes in India. E-commerce regulations and laws in India are limited in nature and this does not allow use of ADR mechanisms and technology driven solutions. For instance, while European Union and other nations are increasingly using online dispute resolution (ODR) for resolving many aspects of e-commerce disputes yet online dispute resolution (ODR) in India is still not known.

Similarly, establishment of e-courts in India can also facilitate early and effective e-commerce disputes resolutions in India. However, till October 2012 we are still waiting for the establishment of first e-court in India. E-courts and ODR in India are urgently required to reduce backlog of cases and for reducing increasing pressure upon traditional courts. E-courts and ODR can also help in e-commerce disputes resolutions in India.

4.13 Misuse of ODR

When records are wantonly accessible, there is a risk of invasion of privacy or misuse of information. Technology must continue to adapt to an environment in which challenges to privacy and the security of information are commonplace. The resolution of disputes online may present new challenges to the security of confidential information. One of the biggest technological obstacles to overcome is the lack of personal connection inherent in conducting a court or ODR proceeding electronically.

4.14 Importance of trust and security on Cyberspace

Information and communication technologies (ICTs) today have impacts on virtually every aspect of society and every corner of the world in information or digital age fostering commerce, improving education and health care, and facilitating communications among all stakeholders. The more cases of cyber- crimes over the ICTs especially through the fastest growing medium like Internet, the more voices for regulating them in any

Notes

pattern. Some countries, thus, began to accommodate such voices or demands through revising the existing laws and / or issuing new legislation(s) – or—'cyber-laws' to deal with new issues on ICTs.

The term or scope of—'cyber-laws' is yet unclear in many countries although it can be interpreted at large in two: One is for the relevant le gislations dealing with or regulating converged computer, telecommunications and multimedia or broadcasting in such cases as the Multimedia and Communications Act, Malaysia; the other is for those tackling the emerging cyber-crimes in such cases as the Information Technology Act in India and the Convention of Cyber-crimes adopted by the Council of Europe. The term of cyber-laws or legislations referred to in this paper will be limited to the latter.

In the global information society – beyond national jurisdictions, an escalating national de jure regulation meets a similarly pervasive de facto futility of enforcement. National legislatures might continue to enact regulations especially over criminal matters, but their regulatory endeavors are unlikely to be effectively enforceable, as they desire due to the global nature of ICTs. Global phenomena like cyber-crimes should in principle propel nations to achieve legislative co-operation and partnership at international levels, since cyber-space is no respecter of national boundaries. The nature and extent of the problem in enforcing the laws over the cyberspace is enormous. Some law enforcement agencies are responding aggressively, others are not fully aware of the problem on the cyberspace and lack the expertise and resources to pursue the kind of cases appearing every day. Some ISPs have taken affirmative action's to crackdown on cyber offenders, whilst others have not. There is a great deal more that government and/or industry can and should do to empower individuals to protect themselves against cyber offenders and other online threats.

4.15 Scope and Development of Cyber Laws

The existing legislations and statutes need to be reviewed to determine whether they can address the issues arising out of the new ICT era. If the current laws are inadequate to deal with the problems, national governments and / or appropriate regional and international bodies need to either revise the existing laws or enact new laws to provide individual, corporate and government users with maximum trust and security, as Table 4.1 articulates a few examples.

Enforcement mechanisms to optimize benefits of ICTs and secure confidence of users, information society should be safe and secured through not only cyber-laws per se but also appropriate enforcement mechanisms. However, first of all, many countries do not have specific enforcement agencies to combat various cyber-crimes.

Notes

Table 4.1: Scope and Development of ICT Legislations

Issues	Laws	National Actions	International Actions
Contracts	Electronic Transaction Act	Hong Kong/ China, Singapore, Thailand etc.	UNCITRAL: Model Law
Harmful sites or contents	Penal Law or Legislation, Obscenity Law, Communication Decency Act, Obscene Publication Act, Self-regulation etc.	Australia, China, HK/China, India, Japan, Malaysia, New Zealand, Philippines, Singapore etc. Hong Kong/China, USA, UK, EU etc.	N.A.
Hacking & virus	E-Commerce Act	Philippine	N.A.
Intellectual Property Right (IPR)	Copyright Law, Patents Law, Trade Marks Law, IPR Law, Green Paper on Counterfeiting & Piracy etc.	Hong Kong/China, S.Korea, Singapore, India, EU etc.	WIPO: Ratification
Data protection & privacy	Personal Data Law Privacy Law, Directive, Self-regulation etc.	Hong Kong/China, S.Korea, EU(e.g.,D95/46/ EC) USA etc.	OECD: Guidelines on Trans-border Data Barriers & The Protection of Privacy
Security	Electronic Transactions Act, Digital Signature Laws, Standards IT Act etc.	Hong Kong/China, Germany, Italy, Malaysia Singapore etc. UK (e.g., BS7799) India	ITU: Recommendations ISO: Standards
Taxation	Internet Tax Freedom Act etc.	USA etc.	N.A.
Domain names	N.A.	Adopt ICANN practice in many nations.	ICANN

Consumer protection	Extension of existing consumer protection Act	EU etc.	N.A.
SPAM	Spam Bill (2003)	Australia, EU & USA	ITU: New initiative (2004)
Beyond national jurisdiction	N.A.	N.A.	ITU & ISO standards EU: Cyber-crime Treaty (2002)

It is only the recent when countries started to create such agencies. For instance, a Cyber-crime Agency called European and Network Information Security Agency (ENISA)' was created in early 2004 with a final approval by the European Union. The National Cyber Security Center (NCSC) was set up under the wing of the National intelligence Service (NIC) in South Korea in 2004. Whilst, Operation Cyber Seep in the USA is being coordinated nationwide between the Justice Department, the Federal Bureau of Investigation, the Federal Trade Commission, postal inspectors and customs agents with supported by state authorities and foreign government' – i.e., close coordination is required among relevant agencies at not only national levels but also regional and global levels, since one of the most important challenge often faced by the enforcement agencies is that the cyber-criminals have the ability to commit the crime quickly and then disappear without revealing their true identity or location.

Often these criminals are located in a foreign jurisdiction. Thus, tracking them requires law enforcement agencies to be created and act faster through cyber border cooperation from a spectrum of organizations representing governments, businesses and consumer groups in various countries.

Second, cyber-law enforcement is relatively a new challenge for the most enforcement agencies. Many countries do not have necessary skilled law enforcement personnel to deal with computer and even broader ICT related crimes. This undercuts the efforts to battle the growing threats like cyber-crimes. In this regard, some countries have started special training for cyber policemen in India by the Ministry of Communications and Information Technologies and Anti-Cyber Crimes Cell (ACCC) officials in Pakistan. Many others are still developing their expertise and resources to investigate and prosecute cyber cases. Third, according to a recent survey of law enforcement agencies, it appears that a majority of the agencies have not investigated or prosecuted any cyber cases. The reason for such laxity was attributed to mainly the fact that the majority of its victims don't report the conduct to law enforcement agencies. Moreover, the law enforcement agencies per se will not take them seriously: i.e., lack of awareness of importance of

Notes

enforcement on cyber-crimes. Most law enforcement agencies do neither recognize the serious nature of the cyber cases and nor investigate them. This requires for raising awareness and education from not only the enforcement agencies but also victims and citizens at large.

Fourth, at national levels, several countries began to impose legal enforcements such as penalties or imprisonments on different types of cyber-crimes. For example, according to the Spam Law passed on December 2 2003 in Australia, first offenses will result in a maximum penalty of US$161,000 per day for organizations and US$32,200 per a day for individuals. Repeat corporat offenders will face a maximum penalty of US$805,500 for each day of spamming, with individuals who are repeat spammers facing a maximum penalty of US$161,000 per day.' In case of Singapore, violators of the Computer Misuse Act such as website crackers can be jailed up to 3 years of fined up to S$10,000'.

Fifth, greater cooperation, harmonization and effective communications among law enforcement agencies and relevant bodies at national, regional and international levels are essential to combat sophisticated cyber-crimes or unlawful conducts at different jurisdictions through the ICTs, especially on the Internet, since the limitation of law enforcement agencies to specific geographic jurisdictions creates serious challenges for them when they investigate activities that can be readily contrived to be extra-jurisdictional (i.e. occur somewhere else), trans-jurisdictional (i.e. occur across two or more areas), or are supra- jurisdictional (i.e. occur somewhere that no agency has jurisdiction over). To meet this challenge of cross-border cyber-crimes at regional and international levels: e.g.

- EU issued the Cyber-Crime Treaty in 2002, which has been signed by the major European countries. Its main principle was based on a uniform approach to fight the cyber-crimes to deal with jurisdiction and enforcement.
- ASEAN countries also seek stronger security links through a consideration to develop a treaty on cyber-crime, so is the commonwealth.
- OECD developed a new web site www.oecd.org/sti/cultureofsecurity dedicated to help combat security risks to information systems and networks.
- UN ESCAP organized a seminar on—Harmonized Development of Legal and Regulatory Systems for E-Commerce in Asia and the Pacific to raise awareness among lawyers, justices, and legal professionals.
- ITU as the mandates has taken various actions from developing international standards to organizing numerous seminars and meetings in order to build confidence and ensure security of ICT, especially its networks.

Sixth, another important enforcement mechanism can be community or industry self-regulation such as code of conducts or practices: e.g., the USA – especially the FCC - together with private industries is in favor of 'un-regulation' of Internet markets or 'self-regulation' by industries themselves especially in the areas of privacy or personal data protection. Last but not least, law enforcements should be hand-in-hand with developing technical measures such as software (e.g., open-source e-mail software, filtering system) and hardware (e.g., a new—chip and pin card).

4.16 Future Aspects

The more cases of cyber-crimes over the converged ICTs especially through the growth of Internet and e-commerce beyond national boundaries, the more voices for regulating them at national, regional and international or multi - lateral forms. As the types of cyber-crimes vary, however, ways of tackling the different types of cybercrimes especially through legislations or regulations may diverse from one country to another, especially when they occur within a specific national jurisdiction with different definitions and socio-political environments from others. Thus, harmonization of the relevant or different national laws is increasingly required, which has been recognized and taken up actions by UN agencies like the ESCAP and ITU. As well demonstrated in such cyber-crimes as—'love virus' or—'cyber-attack' affected by more than one national jurisdiction, there is also need for either bi-lateral or multi-lateral cooperation on the prosecution of international hackers or criminals to go farther and possibly include a cyber-law treaty as practiced by the EC.

As a matter of fact, international legal instruments, which by definition embody global consensus and/ or bind all member nations, could provide countries with useful and creative tools for specific and defined areas of cyber-crimes as international enforcement mechanisms: e.g., global conventions, multilateral treaties (e.g., the Cyber-crime Treaty in the EU), international laws, global standards (e.g., ITU and ISO) for confidence and security, model uniform laws (e.g., UNITRAL), and model contracts/standard terms.

Recognizing the need for confidence and security in the use of ICTs at a global level, moreover, the World Summit on the Information Society (WSIS) led by the ITU in 2003 has adopted that. A global culture of cyber security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation' in declaration of its principles. The WSIS has also adopted the Plan of Action including that governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: considering legislation that allows for effective investigation and prosecution of misuse; and encouraging education and raising awareness.

Notes

In view of the fact that cyber-crimes are growing at alarming rate, each country by all stakeholders needs to have more pragmatic approaches at national, regional and international levels: e.g.,

- Raise awareness of serious nature of the cyber-crimes for various target groups from individuals, industries, and governments to specific enforcement agencies.
- Revise, enact and enforce national and international laws specifying various substantive and procedural aspects of issues emerging from cyber-space: i.e., cyber-crimes.
- Harmonize different national laws to regulate and police the cyber-crimes in a consistent and collective manner at various jurisdictional aspects.
- Coordinate and cooperate between and among the law enforcement agencies of one's own country as well as other countries concerned.
- Endeavor to establish International Tribunals to regulate cyber cases or crimes increased beyond national jurisdictions.

To sum up, every stakeholder should be aware of and actively involved in preventing and solving together the destructive side of ICTs - i.e., cyber-crimes - with an appropriate balance between regulations and self-regulations subject to the different types of crimes in cyber-space, in order to optimize more creative side or benefits of ICTs, which will further transform the paradigms of our cultures, politics, and socio-economy beyond national jurisdictions in the interconnected world today.

4.17 Misuse of Law Enforcement Agencies

The law enforcement fraternity has never been one for openness and consistency. As the study notes, misuse of the DVS system is handled differently by every law enforcement agency, if it's even punished at all. The lack of a codified "best practices" or even a basic "user agreement" that holds the individual officer responsible for his actions has led to widespread misuse. There is urgent need to resolve this issue.

4.18 Convention on Cyber Crime Treaty

In 1997, the Council of Europe (CoE), an organization of 47 European countries, appointed a Committee of Experts on Crime in Cyberspace to identify and define new crimes, jurisdictional rights and criminal liabilities concerning the Internet. Canada, Japan, South Africa and the U.S. were also invited to participate in the discussions as observer nations. The goal was to create a set of standard laws concerning cybercrimes for the

Notes

global community and create a common criminal policy to protect against cybercrimes. The country representatives sought to make it easier for law enforcement to cooperate in collecting evidence in investigating computer crimes.

The resulting Convention on Cybercrime of the CoE was passed in June 2001 and is currently the only global document on this issue (CoE, 2001).

The document attempts to define cybercrimes and to develop policies to prevent particular crimes committed with use of the internet. The treaty includes provisions geared toward fighting terrorism, child sexual exploitation, organized crime, copyright infringement, hacking, and internet fraud. The Convention also acts as a framework for international cooperation between countries in investigating and prosecuting possible cybercrimes. Other portions of the treaty include descriptions of extradition procedures.

If countries agree to the treaty, they must agree to pass legislation to address particular computer crimes. They also agree to provide international cooperation to other parties in the fight against computer-related crime by providing a contact for countries that need immediate help in investigating a computer crime (Boni, 2001). The treaty gives police agencies expanded powers to investigate and prosecute computer crimes when the offense crosses national borders (US Ratifies, 2006).

On November 7, 2002, the Council of Ministers adopted an additional protoco l, separate from the main Cybercrime Convention, which addresses racist and xenophobic materials committed through computer networks (CoE, 2001).

After the CoE finalized the proposed treaty, it was signed by twenty-six member states in Budapest, Hungary. The countries who enjoyed observer status' (the U.S., Mexico, Japan, and Canad(a) had the option to sign it. It was then sent to countries for ratification (Hancock, 2000). The treaty came into effect when five states, including at least three CoE member states, ratified it (Convention on Cybercrime Update, 2002).

The Convention entered into force on July 1, 2004. To date, the Convention has been ratified by twenty-four countries; twenty-three of whom have also signed it but not ratified it. The last country to ratify the treaty was Germany, which did so on March 9, 2009. The U.S. Senate ratified the treaty on August 3, 2006. Although it appears to be a significant policy to attack cyber criminals, when examined closely, it is clear that the treaty has many elements of symbolism in it.

The Treaty is organized into four chapters. Each chapter includes different sections, which are then broken down into articles. Each chapter discusses a different aspect of the treaty, with specifics given in the articles. In all, there are 48 articles in the treaty.

4.19 Approaches against Cybercrime

Notes

In order to set the stage for the discussion of the individual countries that follow it is important to note that most countries do not act unilaterally on issues related to cyber-space (and indeed on any issue with international aspects). However, countries do act traditionally, by definition, on domestic issues within their jurisdiction. Part of the difficulty of formulating cyber-strategies and cooperating in cyberspace is that it is not always clear whether a threat to computers or networks or to personal information is domestic, or international, in origin.

To illustrate this difficulty, consider the following Origins of Hacks' map, provided by the NCC Group. The map portrays the top ten countries in the third quarter of 2012 that served as the point of origin of an attack on another computer (a ―hack or ― cyber-attack). Some of these attacks, no doubt are aimed at computers and networks in other countries, but others are aimed at computers within the country. Each of these countries, and indeed each and every country that participates in cyberspace, faces the same challenge of attempting to formulate courses of action that integrate both domestic authority and international cooperation. With limited domestic resources, lack of inter-jurisdictional cooperation, and lack of regulatory enforcement in cyberspace, countries have attempted to increase cooperation with other countries and within international treaties.

United States – Australia: In 1951 the Australia, New Zealand, United States Security Treaty (ANZUS) was signed to cooperate on military defence matters in the Pacific Ocean. The Treaty is an alliance of three countries built on separate bilateral bonds – one between United States and Australia and another between Australia and New Zealand.

Since 1985 New Zealand has been an inactive member of the Treaty and the meetings are being held only between U.S. and Australia's officials. In 2011 a new clause was added to ANZUS, which specifies that it will also apply to the cyberspace.

New Zealand – Australia: New Zealand has recently moved from observer status to membership in Australia's Counter-Terrorism and Emergency Management Committees. In a recent joint statement it was agreed that both countries will work together in the cyber incident response area to ensure that networks of national importance remain resilient to cyber intrusions.

New Zealand – United Kingdom: New Zealand and the United Kingdom are preparing an agreement in which the two countries will share intelligence, research and development on internet offences, and will draw common strategic goals. United States – China: bilateral discussions on cooperation in the Cyber security China Institute of

Contemporary International Relations (CICIR, Chin(a) and the Center for Strategic and International Studies (CSIS, United States) started in 2009 and the respected organizations have held six formal meetings on cyber security since that time.

Over the years the parties have reached some areas of agreement and shared views on issues such as risk of third-party' non-state actors (i.e., terrorist groups), and views on cooperation against cybercrimes such as fraud and child pornography.

Meanwhile, the U.S. indicated that the line between civilian and military is blurred, but the concept of the protection of civilians can be found in the Geneva and Hague conventions, which CSIS proposes that all nations agree to observe in cyberspace'. Furthermore, the parties discuss what behaviors could be considered cyber-attack or cyber war. So far they agreed that the stakes should be high; however, they still need to define the duration and effects of cyber actions that could be regarded as cyber-attacks. We have yet to observe what turn the international dialog on cyber security between the two countries will take in light of the recent report from the U.S.-based cyber threat analysis agency Mandiant that exposed a series of cyber-attacks from China on United States, the accusations that where later denied by Chinese officials.

China – France: The China-France Joint Working Committee on Information Technology and Communications.

Furthermore, there is a bilateral China-US engagement On Cyber security Cooperation against Spam' since 2011. The objectives of this cooperation include:

- Establishing a genuine dialogue between the subject matter experts and stakeholders from the two countries;
- Develop common understanding of each other's perspectives;
- Agree on international policy for reducing spam in cyberspace.

United States – Canada: Cyber security cooperation is part of the action plan Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness between the two countries.

United Kingdom – India both countries announced in 2013 that the countries will sign an agreement on cyber security issues this year, which should improve personal data protection and increase the stored amount of United Kingdom's data on Indian servers.

As to international agreements, there are many international bodies that aim to regulate cyberspace. Among the prominent initiatives are those of the United Nations (UN) and the Council of Europe (also known as the Budapest Convention). Most of the European countries are signatories to the Council of Europe Convention on Cybercrime and assign greater focus on multilateral regional alliance rather than on establishing

Notes

bilateral cooperation with some select countries. The Council of Europe Convention on Cybercrime was the first international treaty that focused on legal procedures to address the acts of criminal behavior against computer systems and networks. Apart from the 45 members of the Council of Europe, the Budapest Convention has been adopted by Canada, Japan, South Africa and the United States.

4.20 U.S. Policy

Both the Clinton and Bush Administrations worked closely with the Council of Europe on the Convention. U.S. officials believe that it removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes.

The Bush Administration was pleased with the Convention's data preservation approach, which requires the storage of specified data—relevant to a particular criminal investigation and already in a service provider's possession—for a limited period of time. It views this provision, currently lacking in many national laws, as key to improving the counter-terrorist capabilities of law enforcement officials worldwide.

As noted above, the Bush Administration submitted the Convention to the Senate for ratification in November 2003. U.S. policymakers assert that the Conventi on will not require implementing legislation; the United States will comply with the Convention based on existing U.S. federal law. Legal analysts say that American negotiators succeeded in scrapping most objectionable provisions, such as the hate speech article, thereby ensuring that the Convention tracks closely with existing U.S. laws.

Proponents assert that many of the Convention provisions reflect the spirit of several Congressional measures that relate to cybercrime, cyber terrorism and cyber security, including:

- The USA PATRIOT Act (P.L. 107-56, introduced as H.R. 3162 by Rep. James Sensenbrenner in October 2001) authorizes the interception of electronic communications for the collection of evidence related to terrorism, computer fraud, and abuse (Sections 201 and 202). It also clarifies the definition of protected computers and increases fines and prison terms for damage (Section 814).
- The Homeland Security Act (P.L. 107-296 introduced as H.R. 5005 by Rep. Richard Armey in June 2002) directs the U.S. Sentencing Commission to reevaluate federal sentencing guidelines for crimes involving computer-related fraud and hacking offenses, especially against restricted federal government systems (Section 225, the Cyber Security Enhancement Act of 2002).

4.21 The United Nations (UN)

The UN attempts to govern cyberspace through the International Telecommunications Union (ITU) and the regulations created by the ITU (ITRs). The United Nations Office for Drugs and Crime (UNODC) is also concerned with cybercrime. ITRs concerning cyberspace were adopted initially in 1988. A resolution on computer crime legislation was adopted in 1990, at the 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba. In 2000 Resolution 55/63 on combating the criminal misuse of information technologies was adopted by the General Assembly, and it includes the following statements:

- States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.
- Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.

This was followed by Resolution 56/121 in 2001, and by the launch in 2007 of the Global Cybercrime Agenda (GCA) by the ITU. In 2010 the General Assembly adopted Resolution 65/230 that proposed to establish an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the 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 latest amendments (Final Acts') were added to the ITR at the recent World Conference on International Telecommunication held in Dubai in December 2012 (WCIT-12). 89 countries were signatories to the Final Acts. Among the countries covered in this report, only Russia signed the amendments, and the Dubai amendments were widely portrayed as attempts by Russia and its allies to wrest control over the internet from the United States.

4.22 The Council of Europe (Budapest Convention)

The Council covers Europe as well as Russia. Canada and the US are Observer States. In 1997 the Council established a Committee of Experts on Crime in Cyber-space, and in 2001 the Council adopted the Convention on Cybercrime, known as the Budapest Convention.

Russia objects to certain Convention provisions, which allow for what Russia considers extra jurisdictional exercises of power that amount to interference in a country's internal affairs. According to some reports over 100 nations are using the Council of Europe Convention as the basis for domestic legislation to combat the threat

of cybercrime. So far 35 countries are a party to the Convention. Other prominent organizations include the OECD, NATO and APEC.

Notes

4.23 The Organisation for Economic Co-operation and Development (OECD)

The OECD was the first international organization that initiated guidelines for computer crime. By its nature the OECD does not establish treaties, and it is devoted to the promotion of a global coordinated policy approach. The OECD established a Task Force on Spam in 2004 The OECD Working Party on Information and Privacy (WPISP) develops international guidelines on cyber security and in 2002 published a document titled Security of Information Systems and Networks: Towards a Culture of Security. In 2008 it released Scoping paper on online Identity theft' a report with some recommendations on how to fight identity theft (this document also suggested to recognize identity theft as a separate offence in criminal laws.) It was followed up in 2009 by the OECD Policy Guidance on Online Identity Theft' report.

4.24 The North Atlantic Treaty Organization (NATO)

By virtue of its mandate NATO focuses more on cyber-attacks carried by countries or national elements against NATO members. NATO's Senior Civil Emergency Planning Committee (SCEPC) assists NATO members in the protection of civilian populations from terrorist attacks against critical infrastructure and is also responsible for coordinating the civil critical infrastructure. NATO's Civil Communication Planning Committee (CCPC) is responsible for the electronic public and non-public communication infrastructures, and has published several papers on civil communications infrastructures. NATO's Civil Protection committee (CPC) has initiated work on critical infrastructure protection, and developed a Critical Infrastructure Protection Concept Paper in 2003. NATO's Industrial Planning Committee (IPC) has also contributed on preventive measures for the protection of critical infrastructure. NATO established a Centre of Excellence for Defense against Terrorism in 2008.

4.25 Asia Pacific Economic Cooperation (APEC)

The deliberations of APEC are important in this and other multinational areas since it brings together the US, Canada, China and Russia. In 1990 APEC established its Telecommunications and Information Working Group (TEL) that works in turn through three groups: the Liberalization Steering Group (LSG), the ICT Development Steering Group (DSG) and the Security and Prosperity Steering Group (SPSG). . SPSG's scope covers the promotion of security, trust and confidence in networks/ infrastructure/

services /technologies/applications/e- commerce; oversight of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs); the issues of Spam, Spyware and Cybercrime prevention; the development of human resources and capacity in order to combat cybercrime and implement effective cyber security awareness initiatives; and the facilitation of business through discussions with the private sector on promoting security, trust and confidence in the use of ICT for business and trade. Of these, the e-Security Task Group created in 2003 a Cybercrime Legislation & Enforcement Capacity Building Project.

Two other multinational organizations should also be mentioned. The Organization of American States (OAS) to which both Canada and the US belong, has a Department of Legal Cooperation that offers an Inter-American Cooperation Portal on Cyber-Crime'. OAS agreed in 2003 to a Comprehensive Inter-American Cyber-security Strategy: A multidimensional and multidisciplinary approach to creating a culture of Cyber-security.

The Shanghai Cooperation Organization (SCO) is an organization of Russia, China and several former Soviet republics. These countries have entered into the Shanghai Convention on Combating Terrorism, Separatism and Extremism. SCO has also issued several related statements: The Yekaterinburg Declaration of 2009 mentioned information security as one of the main priorities in a common system of international security. In 2012 SCO's Heads of State Council meeting in Beijing stated: The SCO will stand firm to fight against terrorism, separatism and extremism as well as international cybercrime.

Sometimes international cooperation against cybercrime is established with a very particular goal and not just on a national level but between specific governmental agencies. An example of such organization is The Virtual Global Taskforce (VGT).

4.26 The Virtual Global Taskforce (VGT)

VGT is an alliance of international law enforcement agencies and private sector partners working together to combat online child sexual abuse. Specifically, the VGT comprises the Australian Federal Police as Chair, the Child Exploitation and Online Protection Centre in the UK, the Royal Canadian Mounted Police, the US Department of Homeland Security, INTERPOL, the Italian Postal and Communication Police Service, the Ministry of Interior for the United Arab Emirates, the New Zealand Police and Europol.

One more particularly notable international organization against cybercrime is Strategic Alliance Cyber Crime Working Group.

4.27 Strategic Alliance Cyber Crime Working Group (SACCWG)

SACCWG was assembled in 2006. It is a special unit consisting of five law enforcement agencies: The Australian High Tech Crime Centre (AHTCC), FBI (USA), New Zealand

Police, Royal Canadian Mounted Police, and Serious Organized Crime Agency (United Kingdom). Over the last five years several countries repeatedly tried to initiate discussion about the need for common international Cyberspace Treaty, suggesting that bilateral and regional agreements are not enough to secure cyberspace and prevent cyber-war.

Notes

4.28 Misuse of International Conventions

The Conventions and their Additional Protocols contain several articles on the emblem. Among other things, they specify the use, size, purpose and placing of the emblem, the persons and property itprotects, who can use it, what respect forthe emblem entails and the penalties for misuse. According to studies in peace and conflict resolution, the relative importance of diversion or misuse of offici ally authorized transfers compared to international illegal black market trafficking has been thoroughly confirmed and the author here goes on to elaborate that for most developing or fragile states a combination of weak domestic authorized firearms possession with theft, lost or corrupt sale tends to be a big source.

4.29 Summary

ODR is a wide field, which may be applied to a range of disputes; from interpersonal disputes including consumer to consumer disputes (C2C) or marital separation; to court disputes and interstate conflicts. It is believed that efficient mechanisms to resolve online disputes will impact in the development of e- commerce. ODR is a highly recommended method because it is not as time consuming as normal litigation, disputes are easily documented and the person need not submit to the jurisdiction of any court.

The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe. Until recently, many information technology (IT) professionals lacked awareness of an interest in the cybercrime phenomenon.

A cybercrime can play havoc in cyberspace if it is a bot attack. As the speed of committing crime and impact thereof is greater in cybercrime cases and because electronic evidence can be easily tampered or is volatile, it is imperative to trace the offender in the shortest possible time and preserve original evidence. Moreover, tracing of offender in cybercrime cases may be more difficult due to availability of several techniques to camouflage one's identity using steganography, onion routing or other hide IP practices.

4.30 Review Questions

1. Describe the nature of ODR.
2. Discuss why ODR is important.
3. What are the drawbacks of ODR?
4. What all are the benefits of ODR?
5. Explain the difference between ODR and litigation.
6. What are the various pragmatic approaches at national, regional and international levels for cybercrime?
7. How challenges of cross-border cyber-crimes are faced at regional and international levels?
8. Discuss any two international conventions on cybercrime.
9. What are the future aspects of enforcement agencies against cybercrime?
10. Discuss some areas where development of cyber laws are must.
11. Write a short note on conventions on cybercrime.
12. What are the approaches of different countries to combat against cybercrime? Explain any three.
13. Write a note on OECD.
14. How U.S. policy and U.N. policy differs with each other?
15. What do you understand by NATO and APEC? Explain.

4.31 Further Readings

- A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime
- Introduction to Indian Cyber Law by Rohas Nagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf
- Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
- Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
- Cyber Forensics in India; retrieved from http://perry4law.org/cfii/
- Digital Evidence & the Indian Law by Asian School of Cyber Laws; retrieved from http://www.asianlaws.org/del.pdf