Course : PGDCL-01

Vardhaman Mahaveer Open University,
Kota

Cyber Space Jurisprudance

Course Development Committee **PGDCL-01**

Chairman

Prof. L. R. Gurjar

Director (Academic)

Vardhaman Mahaveer Open University, Kota

Convener and Members

Convener

Dr. Yogesh Sharma, Asso. Professor
Department of Law
Vardhaman Mahaveer Open University, Kota

Prof. H.B. Nanadwana
Director, SOCE
Vardhaman Mahaveer Open University, Kota

External Members:

1. Prof. Satish C. Shastri
Dean, Faculty of law, MITS, Laxmangarh
Sikar, and Ex. Dean,
University of Rajasthan, Jaipur (Raj.)

2. Prof. V.K. Sharma
Deptt.of Law
J.N.Vyas University, Jodhpur

3. Dr. M.L. Pitaliya
Ex. Dean, MDS University, Ajmer
Principal, Govt. P.G.College, Chittorgarh (Raj.)

4. Prof. (Dr.) Shefali Yadav
Professor & Dean - Law
Dr. Shakuntala Misra National
Rehabilitation University, Lucknow

5. Dr Yogendra Srivastava, Asso. Prof.
School of Law,
Jagran Lakecity University, Bhopal

Editing and Course Writing

Editor:
Dr. Yogesh Sharma
Convener, Department of Law
Vardhaman Mahaveer Open University, Kota

Course Writer:
Dr Kusum Dixit
Principal & HOD, School of Law
AISECT University, Bhopal

Academic and Administrative Management

Prof. Vinay Kumar Pathak
Vice-Chancellor
Vardhaman Mahaveer Open University, Kota

Prof. L.R. Gurjar
Director (Academic)
Vardhaman Mahaveer Open University, Kota

Prof. Karan Singh
Director (MP&D)
Vardhaman Mahaveer Open University, Kota

Prof. H.B. Nanadwana
Director, SOCE
Vardhaman Mahaveer Open University, Kota

Course Material Production

Prof. Karan Singh

Director (MP&D)

Vardhaman Mahaveer Open University, Kota

Production 2015 ISBN-978-81-8496-576-6

Vardhaman Mahaveer Open University, Kota
Cyber Space Jurisprudance

Unit-1
Introduction to Cyber Space
(Meaning & Evolution)

OBJECTIVES:

After going through this unit you should be able to Understanding the meaning of cyber space

- Understanding the jurisprudence of Indian cyber law in cyber space
- Understanding the need for cyber law in cyber space

Structure:

1.1 Introduction[1]

Lot of us have a limited knowledge of crime occurring in "cyberspace", known as cyberspace, which happens on computer and the Internet, however, cyberspace has a severe potential for remarkable impact on the lives of individuals and our society. Therefore, a detailed introduction of cyberspace

[1] A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/

needs to be presented. There are many terms used to describe cyberspace. 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. 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 cyberspace, 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 cybercrime, since other fields also have "hi-tech" developments like nanotechnology and bioengineering. Currently, although no one term has become totally dominant in use, "cyberspace" is the term used most pervasively. In general, cyberspace has three categories:

1. Target cyberspace: the crime in which a computer is the target of the offense.
2. Tool cyberspace: 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 cyberspace is short compared with traditional crimes. The first published report of cyberspace 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 cyberspace were always "insider" cyberspace, 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 cyberspace 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 in cyberspace. 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.

1.2 Origin of Cyber space[2]

It is believed the first recorded cyberspace 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 1970ties. 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:

[2] Security, Prevention and Detection of Cyber Crimes by Asherry Magalla, Tumaini University Iringa University College; retrieved from http://www.academia.edu/3471542/THE_INTRODUCTION_TO_CYBERCRIME_SECURITY_PREVENTION_AND_DETECTION_OF_CYBERCRIME_IN_TANZANIA

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

1.3 What is Cyber Law in cyber space?[3]

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?

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.

[3]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

- 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.

1.4 Need for Cyber Law in cyber space[4]

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.

[4] Introduction to Indian Cyber Law by RohasNagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf

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.

1.5 Jurisprudence of Indian Cyber Law in cyber space[5]

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

[5] 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

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 16thDecember 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.

1.6 Introduction to Cyber Crime in cyber space[6]

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.

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

[6]Introduction to Cybercrime (.pdf); retrieved from http://webcache.googleusercontent.com/search?q=cache:UuufsIlO0FQJ:wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%2Bcrime.pdf+&cd=1&hl=en&ct=clnk&gl=in

threatened. They committed acts of sabotage ego discourage Jacquard from further use of the new technology. This is the first recorded cybercrime.

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. Cybercrime 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

1.7 Defining Cyber Crime in cyber space[7]

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

[7]Introduction to Cybercrime (.pdf); retrieved from http://webcache.googleusercontent.com/search?q=cache:UuufsIlO0FQJ:wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%2Bcrime.pdf+&cd=1&hl=en&ct=clnk&gl=in

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.

1.7.1 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.

1.7.2 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'.

1.7.3 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.

1.7.4 Intellectual Property crimes

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

1.7.5 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, 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.

1.7.6 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.

1.7.7 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 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.

1.7.8 Cyber stalking

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.

1.8 Frequently Used Cyber Crimes in cyber space[8]

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

[8]Introduction to Cybercrime (.pdf); retrieved from http://webcache.googleusercontent.com/search?q=cache:UuufsIlO0FQJ:wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%2Bcrime.pdf+&cd=1&hl=en&ct=clnk&gl=in

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 amount of money (say Rs. 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 the14th 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.

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 ora peripheral attached to the computer.

Physically damaging a computer system

This crime is committed by physically damaging a computer or its peripherals.[9]

1.9 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

[9] Introduction to Cybercrime (.pdf); retrieved from http://webcache.googleusercontent.com/search?q=cache:UuufsIlO0FQJ:wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%2Bcrime.pdf+&cd=1&hl=en&ct=clnk&gl=in

cyberspace was clutching up which gave birth to cybercrimes at the domestic and international level as well.

1.10 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.

1.10 References

1) A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/
2) Security, Prevention and Detection of Cyber Crimes by Asherry Magalla, Tumaini University Iringa University College; retrieved from http://www.academia.edu/3471542/THE_INTRODUCTION_TO_CYBERCRIME_SECURITY_PREVENTION_AND_DETECTION_OF_CYBERCRIME_IN_TANZANIA
3) 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
4) Introduction to Cybercrime (.pdf); retrieved from http://webcache.googleusercontent.com/search?q=cache:UuufsIlO0FQJ:wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber%2Bcrime.pdf+&cd=1&hl=en&ct=clnk&gl=in

1.11 Check your progress

1. Cyber Law is the law governing _____.
2. Cybercrimes are _____ acts where the computer is used either as a _____or both.
3. Electronic signatures are used to authenticate_____.
4. CRAT refers to _____.
5. _____ are one type of electronic signature.

6. Information Technology Act, 2000 (IT Act) which came into force on _____.

1.12 Answers to check your progress

1. Cyber space
2. Unlawful/ tool or a target
3. Electronic records
4. Cyber Regulations Appellate Tribunal
5. Digital signatures
6. 17 October 2000

1.13 Terminal 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.

Unit-2

Jurisprudence of Cyber Space: Global Perspective (Part-I)

OBJECTIVES

After going through this unit you should be able to:

- Understanding the difference between cybercrime and conventional crime.
- Understanding the modes and method of cybercrime.
- Understanding the classification of cybercrime and motive behind the attack.

Structure

2.1 Introduction:

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 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".[10]

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.[11]

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

[10] A Survey of Cybercrime by Zhicheng Yang, retrieved from ttp://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/

[11] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

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.[12]

2.2 Conventional Crime in Cyber Space[13]

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.

2.3 Cyber Crime in Cyber Space[14]

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 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.

[12] A Survey of Cybercrime by Zhicheng Yang, retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/

[13] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

[14] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

2.4 Distinction between Conventional & Cyber Crime[15]

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.

2.5 Reasons for Cyber Crime in cyber jurisprudence[16]

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.

[15] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

[16] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

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.

2.6 Cyber Criminals[17]

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 behaviour 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.

2.7 Mode and Methods of Committing Cyber Crimes in cyber space[18]

[17] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

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.

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.

[18] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

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.

2.7 Motive behind any Attack[19]

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.

2.8 Classification of Cyber Crime in cyber space jurisprudence[20]

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

1. Against Individuals

a) Their person &

b) Their property of an individual

2. Against Organization

a) Government

b) Firm, Company, Group of Individuals.

[19] India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both"- In Indian Legal Perspective, by Rajkumar Dubey, retrieved from http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both

[20] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

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.
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

2.9 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

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.

2.10 Relevant Cyber Crimes other than IT Act, 2000

Cybercrimes other than those mentioned under the IT Act[21]

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

[21] India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both"- In Indian Legal Perspective, by Rajkumar Dubey, retrieved from http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both

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

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 Rs 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.

2.11Misuse 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.

COMMISSION OF CYBER CRIME

Most of the cyber-crimes are committed through internet except few in which the malicious data or the protected data is shared, distributed or accessed through non-networking means. Person committing these crimes is well-versed with the technology. The victim or the targeted victim is not in all cases a person of technical background and therefore easily becomes vulnerable to such crimes. It has been found that usually people are unaware or ignorant towards various fraudulent instruments on internet and hence authorise by themselves the un-authorised access. Once access is granted to the computer system, or any such sensitive personal information of the user; entire data of the system or that sensitive information becomes vulnerable to exploitation. This accessed data can be used for any wrongful purpose. It is left at the disposal of the victim to take any efficient step of prevention and retaliation in these situations.

TYPES OF CYBER CRIME

Cyber-crimes can broadly be classified into three types namely- crime against individual, crime against individual property and crime against an organisation or society. This section will deal with one detailed study of each type of above mentioned crime.

CRIME AGAINST INDIVIDUAL

Cyber Stalking

Recent years have seen a series of "moral panics" regarding information accessible on the Internet and its use for criminal activity. A new form of harassment has increased these days known as stalking. Stalking is when an individual targets his victim and threatens him/her. Some examples of stalking is unwanted telephone calls regardless of content, death threat, walking past the target's home or workplace and sending letters or flowers**.** Cyber stalking is a virtual or electronic form of physical stalking. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly or persistent unwelcome contact with another individual.[iii] Unsolicited e-mail is one of the most common forms of harassment, including hate, obscene, or threatening mail. Other forms of harassment include sending the victim viruses or high volumes of electronic junk mail (spamming).[iv]

A 1999 report from the United States Department of Justice suggests, there might be tens of thousands of cyber stalking incidents each year.[v] Through research it has been observed that high proportion of stalkers previously had some type of intimate relationship with the victims or any form of relationship existing prior to stalking. With such a rapid rate of technological development, internet has created a possibility for the internet users including the cyber stalker to hide their original identity. In most cases of online stalking, offenders use an internet protocol (IP) address and anonymous 're- mailers'; that is, mail serves that purposefully strip identifying information and headers showing where the message came from.[vi]

A cyber stalker can communicate directly with their target as soon as the target computer connects in any way to the Internet. The stalker can assume control of the victim's computer and the only defensive option for the victim is to disconnect and relinquish their current Internet "address".[vii] There had been many cases of cyber stalking reported in India like Manisha Kathuria was stalking Rity Kohli by illegally chatting on a chat website called MIRC using her name, he used obscene, obnoxious language and distributed her residence telephone number, inviting people to chat with her on the phone.[viii] A recent case of Akbar Khatri, who was kidnapped from his school by a paedophilic lady 'chat friend' of his, in order to sell him to child traffickers at Pakistan.[ix] These crimes needs to be stopped, proper manner has to be taken and the internet users especially the youngsters need to be educated about the disadvantages of posting information on the Net.

AGAINST INDIVIDUAL PROPERTY

IPR Violations on Internet-

Intellectual property assets is an important asset for any business which require substantial investment of time, money, and creative input and may or may not be tangible. In the Information Technology age, the protection of Intellectual Property Rights (IPR) requires great attention and dedicated strategy for its protection. IPR protected information including music, computer programs, databases can be easily copied and pirated using instantaneous means of reproduction, publication, and dissemination causing serious financial loss to rightful owners. Traditional principles of Intellectual Property Law which apply to the real world also apply to the virtual world.[x]

There are following branches of intellectual property rights e.g. copyright, patent, trademarks, design, geographical indications etc.[xi] The prime reason for rampant privacy of intellectual property on the internet is because it is very easy to copy proprietary and Intellectual Property protected materials and the anonymity that exists in the cyberspace does not deter a party from using the protected materials without due permission from the owner.[xii] Many laws like, the law of copyright, patent law, trade mark law, law of trade secrets are made to protect original forms of expression and include protection of literary work, music, computer software, sound recordings amongst other categories of works. Every country through some legislation seeks to protect these Intellectual Property Rights of people and entities.[xiii] The very frequent way of infringing Intellectual Property right is through Caching (sometimes known as "mirroring", usually when it involves storage of an entire site or other complete set of material from a source).[xiv]

According to the recent report of the Indian Federation of Phonographic Industry (IFPI), among the top 10 nations where music piracy has reached unacceptable levels are India, China, Brazil, Indonesia and Pakistan.[xv] Under the Indian Law, the Copyright Act, 1957 confers on the author of a work including literary, artistic and cinematographic work the right to prevent a party from unauthorised reproducing, modifying or distributing the copyrighted work.[xvi] The case law in India begins with the 1999 Delhi High Court judgement in *Yahoo!, Inc. v Akash Arora & Anr.* This case dealt with the alleged passing off for the services rendered by a party on the internet through

a domain name. The plaintiff sought a permanent injunction restraining the defendants, from dealing in any services or goods on the internet or otherwise under the trademark/ domain name "*yahooindia.com*" or any other domain name which is identical with or deceptively similar to the plaintiff's trademark "Yahoo!".[xvii]

In a recent ruling in India, *CIT v Oracle Software India Ltd*.[xviii] the court held that duplicating a CD at home may account to privacy and violation of Section 14 of the Copyright Act, 1957. Duplicating is a process of copying data from source medium to a destination medium which has the same physical form. For instance copying a music file from one CD to another is duplication.[xix] The other cases that have been filed under the infringement of Intellectual Property rights are *Acqua Minerals Limited v Mr. Pramod Borse& Anr****[xx]***, *Eicher Limited and Anr. v. Web Link India and Anr****[xxi]***. Many websites today offer freeware installations, sell pirated software copies and engage in other criminal activities. Although many measures have been taken, combating copyright infringements continues to be a major challenge in cyberspace.

AGAINST SOCIETY

Cyber Terrorism-

There exists an interrelationship between terrorism and the internet. The internet came after 1990s when computer services became cheaper, quicker and readily available. The internet came with the main purpose to allow cheap communication. But these days the internet has become a popular medium between terrorist group and individual terrorist to communicate their message of hatred and violence. They use the Internet, encrypted E-mail to plan their acts of terrorism and to spread propaganda. The fear surrounding Cyber Terrorism is that terrorists and criminals penetrate infrastructure computer systems and endanger human lives by disrupting military networks, telecommunications, etc. Cyber terrorist create chaos and anarchy by attacking banking and financial computer networks.[xxii]

Cyber Terrorism may involve the same type of terrorist which may be involved in some other type of terrorist attack. Many a times, even after the penetration, attacks on computer systems go unnoticed and even the attacks are delayed like a bomb timer, which is set to execute at a certain time. Terrorism mainly occurs

where we are more vulnerable, reliant and depends on the system. Nowadays more sophisticated terrorist bombs are on the horizon as computers provide the ability for multiple devices to communicate autonomously. The terrorist may adopt the means of bombing, hijacking, kidnapping a political leader etc. These offences are given a colour of political offence and the objectives sought to free the society from the political, social, economic exploitation of the citizen from the established authority in the state.

In India, Rajiv Gandhi's assassination by female suicide bomber Dhanu was first major accident of suicide attack.[xxiii] We all remember the terrorist attack on Mumbai on November 26, 2008 where the terrorist used the most advanced technology in order to carry out the attacks. They used remailer service to send emails, while maintain anonymity which revealed the sophisticated technologies used by the terrorist to carry out their attacks.[xxiv]Subsequently, it was discovered that all calls which were made to plan the attacks were made by using the Voice over Internet Protocol (VOIP).[xxv]

There have been many attacks by Pakistan as they have bitterness over losing two wars with India over Kashmir issue. The Pakistan Cyber Army hacked into the website of the Indian Institute of Remote Sensing, the Centre for Transportation, Research and Management, the Kendriya Vidyalaya of Ratlam (schools run by the Indian Army)- and the Oil and Natural Gas Corporation of India.[xxvi] On December 15, 2009, computers in the Indian Prime Minister's Office (PMO) and the Ministry of External Affairs in New Delhi were hacked by planting a 'Trojan virus' from a mail purportedly sent from China. The Trojan virus allowed the attackers to access delete the personal Gmail accounts of Government officials.[xxvii] Though India is considered slow in developing corrective measures for curbing web-attack and even has failed many times, still it is making continuous efforts to reduce down the same.

CHALLENGES OF FIGHTING CYBER CRIME

Innovations in IT have led to evolution of new criminal methods. Cyber offenders are using new tools to prevent identification and hamper investigations. The nonfigurative nature of cyber-crime poses tough challenges to prevent it at first place; and then to investigate it. These challenges can be broadly categorised as- General Challenges and Legal Challenges.

GENERAL CHALLENGES

- **Dependency on IT-**

Today we have become slaves to internet services in all aspects of life because everything is available in just a click. Many scholarly intellectual material related to academics is available online. Many financial services including e-commerce and e-banking are online. To bring transparency in governance Governments also uses internet as medium to share with citizens certain information of governance through its official websites. This information can be easily accessed and can be used to commit cyber-crimes.

- **Easy Availability of Crime Devices-**

Only basic equipments are needed to commit Cyber-crime such as- Hardware, Software, and Internet Access.[xxviii] These inputs are available at a very nominal cost. For internet access, offenders try to use services that do not require verified registration. Such services include- Public internet terminals, Wireless networks and Hacked Networks.[xxix]

- **Independence of Location-**

The physical presence of cyber offenders at the site of crime scene is completely immaterial. They can commit it sitting at any part of the world. This is the biggest problem to investigating agencies as it complexes the investigation and makes tracing of offenders very difficult.

LEGAL CHALLENGES

- **Challenges in Drafting a National Law –**

The field of Information Technology is highly dynamic with new innovations and technological development taking place regularly.[xxx] This gives potential offenders a fair chance to develop new types of crimes and widen their area of cyber-attacks. With new types of crimes emerging regularly it becomes difficult to define and codify them into the existing law. Neither it is possible to amend the existing statute each time a new crime is identified. Hence, it becomes extremely challenging to draft a national law that could encompass all possible crimes.

- **Impotency of laws –**

  Cyber laws existing today worldwide are inadequate. Most of them have weak penalties which limit deterrence.[xxxi] Secondly, self-protection remains the first line of defence.[xxxii]Precautionary measures are emphasised than punitive ones. The procedural laws and laws of evidence that govern cyber trails are often found to be inadequate in most countries.

SOLUTIONS TO TACKLE CYBER CRIME

Cyber-crime has become a part of cyber world today. Everyone accessing internet is equally vulnerable to cyber-attacks. It is always wise to us to take precaution rather than seeking remedy. This however does not mean that remedial solutions are of little use. Here, we would like to suggest three types of solutions to cyber-crime.

PRECAUTIONARY SOLUTIONS

Precautionary solutions or pre-crime solutions wherein a user of a computer system or a network is required to do and to omit to do certain acts; the commission or omission of which can make the user an easy target of potential offenders. In brief, these measures help to prevent the commission of crimes at first place. These include-

1. Avoid disclosing any information pertaining to one self to prevent cyber stalking.[xxxiii]
2. Always keep backup of your data so that one may not suffer data loss because of sudden online virus attacks.
3. In case of doubts on credibility of transaction through certain online financial portals, avoid giving any financial information like credit card number, bank account etc to avoid financial frauds.
4. Avoid referring, storing or copying files from unknown or entrusted source such as download from internet or unauthentic e-mail attachments.[xxxiv]

TECHNOLOGICAL SOLUTIONS

Information technology is the mother of cyber-crimes. In other words cyber-crime is nothing more than wrongful use of computer technology. Hence, technological innovations are the primary and perhaps most important tool to

fight cyber crime. Development of new technology to prevent, locate and investigate cyber crimes should be a continuous process. Governments should encourage research in this sector by providing financial support for developing such cyber technologies. Developers of such technologies should be rewarded. Further, cyber experts themselves should not engage in any such wrongful use of technology that could cause any form of suffering to anyone. Efforts should be made gradually to make these positive technologies accessible to all.

LEGAL SOLUTIONS

Law can also act as very powerful tool to fight cyber crime. As the famous "Deterrent Theory of Punishment" says- "penalties or punishment for a crime should be so strict that it prevents the offenders and potential offenders to commit the crime." Same should be the guiding line while drafting punishment for cyber crimes. Further, judiciary should also be extra cautious while dealing with cyber cases in the courtroom. E-courts can also help in speeding the process of justice. Since new types of cyber crimes are emerging, cyber laws should be revised and updated consistently and there must be scope for trail and punishment for any crime that is new to cyber world. Study of cyber laws and cyber jurisprudence should be encouraged among law students so that our country gets better quality of lawyers, judges, and law makers who are well equipped to meet the challenges of illegal practices of cyber world.

STATUTORY PROVISIONS IN INDIA AND ITS ANALYSIS

In India, Information Technology Act, 2000 is the umbrella legislation that provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce."[xxxv]The Act also sought consequential amendments in Indian Penal Code and Indian Evidence Act, Reserve Bank of India Act, 1934 and Banker's Book Evidence Act to make them compatible with this Act.

Till 2000, India's cyber space was unregulated in a way. But with the coming of this act, netizens[xxxvi] have heaved a sigh of relief and a number of their concerns have been the Information Technology (Amendment) Act, 2009**.** The act has been successful in regulating e-commerce in India. It is also a safeguard against cyber-crimes to a large extent but with certain limitations. The I.T. Act deals with various cyber-crimes in chapters IX and XI, 43, 65, 66, and 67 being

the important sections. In the analysis of the act we would restrict ourselves to above said chapters. Few of the observations or loopholes of the statute are-

1. The Act comprises of 94 sections and 13 chapters. But majority of sections deal with the provisions of promoting e-commerce. Cyber offences and its penalty are defined only in two (9 and 11) chapters. Hence, it seems that the primary intent of legislature was to promote and regulate e-commerce and not to prevent and penalise cyber crimes.
2. Under section 79 of the act, Intermediaries are not to be liable under certain cases of cyber crimes. A cyber cafe is also an "Intermediary" hence the obligations under section 79 and the rules framed therein for intermediaries already apply to cyber cafe. These rules for cyber cafes are incomplete and require further rule making by state governments.[xxxvii]
3. Pornography by Indian websites is strictly prohibited by the act but pornography on foreign websites is let loose and nothing is being discussed about it. This gives space to Indian cyber criminals to host their pornography related website's content in foreign shores without being penalised.
4. Police is restricted under Cr PC to search private places. Neither in this act is any special powers provided to police to search private places. Cyber criminals mostly operate from homes, where police cannot search.

CONCLUSION

It is practically impossible to eliminate cyber-crime from cyber world; but it can definitely be prevented. No legislation till now has eradicated any crime completely but they have been successful in preventing them. Similarly cyber-crime also cannot be removed completely by any law but it can be prevented through joint efforts of individual, technology and law. It is the time to make aware ourselves aware about commissions and omissions of certain act while working on internet so that we do not become a victim of any such crime. Technology has given birth to this crime and without it; it's impossible to investigate and control cyber-crimes. Law though currently not well equipped today in India; but can act as a strong deterrent to avoid such crimes.[22]

2.12 Summary

In following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. Since Internet

[22] http://www.lawctopus.com/academike/cyber-space-and-cyber-crime/

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.

2.13 References

1. A Survey of Cybercrime by Zhicheng Yang, retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/
2. Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
3. India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both"- In Indian Legal Perspective, by Rajkumar Dubey, retrieved from http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both

2.14 Check your progress

1. _____ is a kind of offence which is normally referred as hacking in the generic sense.
2. _____ are event dependent programs.
3. _____ is derived from the term hi jacking.
4. _____ 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.
5. The term _____ describes any amateur computer programmer who discovered ways to make software run more efficiently.

2.15 Answers to check your progress

1. Unauthorized access
2. Logic bombs
3. Web jacking
4. Paedophiles
5. Hacker

2.16 Terminal Questions

1. Discuss the character of cyber criminals.

2. What do you understand by conventional and cybercrime? Explain in detail.
3. Describe some relevant crimes which are not discussed in IT Act, 2000.
4. What are the motives behind cybercrime?

Unit-3

Jurisprudence of cyber space: Global Perspective (Part-II)

OBJECTIVES

After going through this unit you should be able to:

- Understand the Jurisprudence of cyber Law.
- Understand the Important jurisdictional issues.
- Understand the virus and its attack.
- Legal perspective and Privacy of mobile phone etc,

Structure

3.1 Introduction:

In the new millennium, the major coups of the 'Techno-Scientific Culture' have resulted a new pad of 'Information Revolution' which has touched socio-

economic organizations and the governmental structure of human beings. The chief tracts of Information Technology are they defeat the geographical, legal and jurisdictional boundaries of a particular sovereign nation; and it is rightly said 'Netizens and web-sites are nowhere and all over the place'. In this context, the "Information Revolution' has created for itself one of the most debated questions i.e. of jurisdiction. Since jurisdiction is the 'sin qua non' of administration of justice, a judgment or order or decree is passed by the court without having the jurisdiction, such judgment, or order or decree can be said as "Coram non-judice" -before a court which has no jurisdiction of the matter or before one who is not a judge, and its invalidity can be set up whenever it is sought to be enforced as a foundation for a right even at the stage of execution or collateral proceeding.

The laws relating to jurisdictional jurisprudence characterizing in the terms of the subject matter, territorial aspects, pecuniary and prescribe aspects have been diluted, and do not answer to the emerging issues posed by the cyberspace referring to the standard test laid down in the past nineteenth century doctrine. To meet the ends of justice, a new brand of jurisdictional jurisprudence has been emerged with startling results as there is little or no domestic legislative recognition of the need to evolve a distinct set of legislations for internet jurisdiction. 'Jurisdiction', according to The Encyclopedia America "is power or authority. It is usually applied to courts and quasi-judicial bodies describing the scope of their right to act. Jurisdiction in the sense of judicial power, often describes the general authority of a court to hear and determine controversies and to carry its judgment into effect. In this abstract sense it does not relate to particular case, but instead refers to the scope of courts, capacity to act within certain geographical boundaries and in connection with various kinds of legal controversies. In a more limited sense, jurisdiction means the power of a court to make valid and binding determination in particular controversy. This kind of jurisdiction relates solely to the court's authority in terms of the specific subject matter and property which are involved in the case under consideration."

Meaning of Jurisprudence:

Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law. Jurisprudence refers to two different things.

A. The philosophy of law, or legal theory

B. Case Law

A. Legal theory does not study the characteristics of law in a particular country (e.g. India or Canada) but studies law in general i.e. those attributes common to all legal systems. Legal theory studies questions such as:

1. What is law and legal system?
2. What is the relationship between law and power?
3. What is the relationship between law and justice or morality?
4. Does every society have a legal system?
5. How should we understand concepts like legal rights and legal obligations or duties?
6. What is the proper function of law?
7. What sort of acts should be subject to punishment, and what sort of punishments should be permitted?
8. What is justice?
9. What rights do we have?
10. Is there a duty to obey the law?
11. What value does the rule of law have?

B. Case law is the law that is established through the decisions of the courts and other officials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws.

Cyber Law and Jurisprudence

As we are talking about Cyber jurisprudence it is pertinent to note the inter-relationship between law and jurisprudence. The term 'law' may be interpreted

in many ways like, one may feel law as command of sovereign (Austin's School of law), other may feel that as, it emerged from the customs, it should be flexible for the common usage The other perception is law is rightness (Ethics) of will, and this can never be enforced by external legislation but must be the free choice of the individual. The others say that law is the science of the totality of the rules for which an external legislation is possible' (Nomology). Therefore, jurisprudence is nothing but set of majority accepted principles of a given society. This analogy is proved in the case how *jus civil* and the *jus gentium* were merged into the broad stream of Roman law, destined to fertilize all the legal systems of the world.

Law cannot function in vacuum it seeks a definite place and people voluntarily abiding to it. If law requires some place to be operated and few individuals consciously abiding to it, then what is the need for recognizing group of individuals as society? And what is the need for making separate rules for their governance? Above all, what makes a group of individuals as society? Is it mere physical existence or is there any other thing that substantiates the matter? The need for resolving these questions has come when we are using the term "cyber society" and thinking about its nature.

The technological inventions made so far have created and developed "products" whereas information technology has facilitated "processes" like process of buying, communicating, sharing ideas so an and so forth. This technology enables people to meet, talk and live in cyberspace in the ways not possible in the real space. The cyberspace is more intimate, accurate and unceremonious. The internet as a medium of communication has grown exponentially with the high participation of individuals facilitating each other with mailing, shopping, sharing online news etc. The ability of online users to interact in sophisticated ways form "virtual communities".

The term 'cyber society' or 'cyber community' is used very insecurely by lawyers and research scholars to refer internet users. But to refer a group of individuals as society or community apart from many other commonalities, the interest (proprietary and personal) of the subjects over the field of operation should also be similar though not identical. Perhaps the reason for the tossing of the coin "cyber society" "cyber community" by the social thinkers is its accessibility to every individual. And this very accessibility paved the way for sharing of ideas, moods and for building of common interests and consensus. Now law has to be built on the premise of this consensus itself.

Law has to identify the common principles, on which the cyber society is working, what norms are governing them? And what customary practices are followed in cyber space? Etc and out of such commonalities like customary practices, cultures, usages and the basic norms, law has to formulate. In the words of Savigny " Law grows with the growth and strengthens with the strength of the people and its standard of excellence will generally be found at any given period to be in complete harmony with the prevailing ideas of the best class of citizens". If this 'prudence', is not shown by the subjects of law then such society will be put to nullity. This nurturing of society, whether virtual or physical, is the job of jurisprudence. Therefore every society has to know the philosophy of law governing it and abide to that. As far as physical society is concerned the jurists like Sir John Austin, Salmond, and Sir Frederick Pollock etc have evolved many schools of thoughts and gave possible propositions to the jurisprudence, but for cyber society, jurisprudence is not yet formulated and is still in the realms of legal academia. But contrary to this the 'cyber society' is more of a reality today than it was ever before. On the one hand the Internet has a stake in the economies of the world while on the other it has gripped popular imagination by providing easy communication, entertainment, leisure and relaxation. The Internet is continually changing the dynamics of the world. The law needs to be alive to this change in society. Roscoe Pound once said, "Legal order must be flexible as well as stable. Law must be overhauled continuously and refitted continually to the change in social life which it is to govern". With that goal in mind, the Indian Parliament went about legislating the first cyber law and christened it the Information and Technology Act, 2000.

The Need of Law in Cyber Society

The purpose of law is in the conflict itself. Where there is no dispute or confrontation of interests there the need for law is nil. And "Conflicts arise when there is something to share" more so when the shared object is scarce. This is as truer of the family or neighborhood as the "Cyber Space". When conflicts arise in Cyber Space, we need "Cyber Laws" to restore order to the society. When we are discussing the emerging field of "Cyber Laws" we need therefore try to understand how and why conflicts arise in the "Cyber World". If the conflicts in cyberspace are not making any substantial difference with the conflicts of physical space then the already existing laws, which are governing the physical space, are highly sufficient to regulate cyber space as well, we need not to go for codification of a separate legislation and for evolving new

principles, but the disputes in physical space and the disputes in virtual space are entirely different in nature. Not to go in detail the matters of Jurisdiction, Proprietorship, liabilities of intermittent parties like ISPs (Internet Service Providers), the doctrine of choice of law, principles of defamation, are all put to scrutiny. To put it more understandably the reason for a separate law is "Law" being a "Code of Conduct declared as the most suitable for a given society", law need to make itself suitable as society changes.

This analogy can be extended to the "Cyber Society" as well. The reason for realizing the need for cyber laws even before cyberspace takes its shape, perhaps, is because of claiming non-cyber rights as cyber rights. As long as the trademark owners were away from the Internet world, there were no domain name disputes. This chaotic period of time would churn fundamental principles of cyber law and lead to the evolution of cyber jurisprudence. We should see that there should not be conflict or overlapping between rights of cyber society and non-cyber society. For instance, the doctrine of adverse position has no role to play in cyber space. Because of this divergent issues involved unless we come up with sound principles of jurisprudence applicable in cyber space even law cannot control the cyber space entirety.

Approach of Law

A fundamental theme running through most cyberpunk literature is that (in the near future Earth) commodities are unimportant. Since anything can be manufactured, very cheaply, manufactured goods (and the commodities that are needed to create them) are no longer central to economic life. The only real commodity is information. With information so fundamental to the business world, the mechanics of business are vastly different from those we know at present. In our current product and service based business world, we are used to dealing with items that can be stamped, traced, taxed, counted and measured. When the primary commodity is information, these attributes no longer apply and the structure of the business world is different. Many people have already recognized this,

It is an admitted fact that one or the other devise, whether ethical (self) or institutional, is needed to regulate any activity carried on in cyber space, but interestingly, one important point is missing from our analysis that is what to regulate? Is it flow of information or is it the place where information is flowing? Or is it the subjects (individuals) who are accessing the information to be regulated? If it is the place, where information is flowing, to be regulated

then invariably law has to attribute some significant legal status to the cyber space and accordingly it has to deliberate upon the character, nature, jurisdiction and functions of the cyber space.

If the subject matter of law are the individuals, as they be in physical space using physical devises itself, already existing laws are suffice to clampdown misuse of IT and to curb technological mal practices. We need not to search terminologies to name the crime committed as well no need of establishing new institutions like cyber police station, cyber cops etc. But the difficulty in this approach is, at times it becomes impossible to trace out individual behind a crime committed and it is impracticable to expect that every cyber offence originate from physical space.

If it is the 'information', which is subjected to the regulation by the law then the horizons of the IT law should be so expended that it deal with production, distribution, dissemination, processing of information as a whole as most of the Communication Acts does in the resent past, like German Information and Communication Services Act (1998) and British White Paper, Proposing the creation of a Cross-media regulatory authority, published in the year 2000 and similarly The Indian Communications Convergence Bill 2000 which does not attribute much difference between the e-mail viewed in television and laptop. This approach of law wither away the concept of cyber crime, cyber theft so on and so forth and perhaps may swab lot of confusion about Information space and help us in understanding the nature of cyber activities. But difficulty in equating laws of information technology with communication regulations primarily is the communications regulations deal information more or less as a 'product' where as the information technology is a process. Overlooking of this significant difference may pose serious problems.

Property – cyber space:

'Proprietary ship' an age-old concept of mankind, has always been brought to discussion, whenever threat to its existence has come. All the time man tried his best to protect his proprietary ship over the things he has access.

This terms is used in dissimilar ways by many schools of thoughts,

1. In its widest sense, includes all the legal rights of a person of whatever description.

2. It includes proprietary rights of a person and not his personal rights

3. In other sense, the term property includes only those rights, which are both proprietary and real.

4. It includes only corporal rights or rights of ownership in material things.

5. It includes greatest rights of enjoyment (Austin)

Though, many jurists tried define property, but nevertheless each definition has its own contextual significance. When it is said that property includes all legal rights, they certainly mean it and that perhaps suits to the then prevailing legal and social conditions. But when the circumstances have changed they went in search more appropriate definition. As is rightly pointed out by Erle J.: " The notion that nothing is property which cannot be earmarked and recovered in detenu or trover, may be true in an early stage of society when property is in its simplest form and the remedies for the violation of it are also simple, but it is not true in a more civilized state when the relations of life and the interests arising therefrom are complicated"

It seems in the wake of Information Technology the proprietary rights of interent users are going to be a complex problem. Questions pertaining to tangibility, intangibility, movability and immovability of cyber property and can web page be sold, leased, transferred, bequeathed, is total alienation is possible or not? So on and so forth are going to occupy center points of 'cyber prosperity jurisprudence'

But by using cyberspace as a metaphor we can resolve most of the problems of cyber proprietary ship. The metaphor universally accepted with regard to property is 'property is bundle of rights' and the central tenet of property jurisprudence is that, property is the legal right to exclude others. To put it more clearly, property rights in the internet are negative rights, they lay what is not jurisdiction rather what is jurisdiction. In other words as long as a computer does not violates the rights of others such computer is said to have been within its jurisdiction. This refers that wherever a computer interacts with other computer transgressing its property lines there and then such computer is said to have violated the legal rights of the others. Therefore it is the violation of legal rights of other that will mark boundaries for proper use.

The primary question that needs to be answered is whether *website* constitutes property or not? Though we do not have any legal pronouncement as on today directly dealing with the nature of the websites, we can consider a website as property because, we refer websites as 'sites' like any other physical place, and

we use the terms like ‘web traveling’, ‘visiting’ etc which in turn establish most of the features of physical properties.

Interestingly the trespass against chattels has also found place in cyber space. In the case of ebay vs Bidder’s edge court emphasized on chattel trespass. In the case of State v. McGraw court held that misappropriation of computer resources could constitute trespass against chattel. In another casethe suit is one for defamation claim under the common law, as well as one for unauthorized accessing of e-mails from the personal e-mail account of the plaintiff. Which is challenged as unauthorized intrusion in the personal domain of the plaintiff. The court held that *an email account would constitute a requisite place*. The court held that as per The Electronic Communications Storage Act, Section 2701 "it is violation for anyone who intentionally accesses without authorization a facility through which an electronic communication service is provided and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system". Court observed that the electronic mail stored on Microsoft’s server is with in the definition of electronic storage.

With this case it is clear that electronic mail stored on Microsoft’s server constitutes property, and invasion of it would constitute violation of rights.

It is clear from the above facts that, well (pre) defined principles of property are applied in cyberspace. But, interestingly the cyber property rights and traditional property rights should not be viewed on same parlance. It seems that the judiciary intends to fit this abstract space in to strict jackets of traditional property principles. To quote one basic reason, cyber space is not a physical space and clear demarcation of public domain and private domain is impracticable which requires lot of judicial maturity.

Cyber invasion

The legal consequences of cyber space invasion are something different. Somebody invaded cyber space to disseminate knowledge, to inform, to facilitate, to govern, to serve etc and the others have invaded cyberspace to unshackle the foundations of most (presumably) secured nations, to hack information stored in a remote computer, to destroy, copy documents kept in a computer, to defraud and to bring financial crisis in the country etc., enlisting the reasons for invasion and kinds of invasions would defeat the ends of our discussion. According to statistics provided, in the year 2012, 625 million were accessing web sites on the internet; the current estimates may cross 700 million

by the end of 2003. So any useful services provided on internet would facilitate nearly 700 million people perhaps no human could physically reach these many people in his lifetime as is rightly pointed out by James Madison " Knowledge will forever govern ignorance, and a people who mean to be their own governors, must arm themselves with the power that knowledge gives. A popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy or perhaps both". But if we look the amount of crime growth, the complaints filed in 2012 are 1,351,897 (3,704 per day) and Complaints filed in the year 2011 are 701,939. It clearly indicates that using computer is plugging to liability itself.

Jurisdiction Issue

The Internet is the personification of the information society. Information is now available at the fingertips of many and this has brought about some amazing changes as to way we communicate. We are living in a unique time in the history of human civilization. The Internet has created a monarchy in which individuals, corporations, communities and all other entities including government can exist within and beyond the borders of nation States in an ever-present manner. Increasingly, people in the information society are becoming involved in on-line services, on-line contracts, electronic commerce, and on-line transactions. Some of the reasons behind this online trend provide quite an insight into the Internets popularity. Apart from the fact that Internet is one of the fastest, cheapest and easiest modes of communication today, it has also made the concept of global society more a reality.

It must be appreciated that almost all the information that is placed on the internet is generally available to anyone who is having an Internet connection. Subscribing for Internet connection now-a-days does not cost much. This allows blanket access to all on-line material. Earlier before Internet, if a person wanted to sell his product, he had limited access to customers and that too by spending exorbitant sum of money for advertisement. Thus geographical boundaries were the major hindrance. Today, a person can sell goods from a desktop computer located anywhere to many different consumers all over the world by means of the Internet.

Along with the unique opportunities the Internet offers, it also poses new and significant challenges to traditional legal philosophy. The growth of trans-border activities poses new challenges for law enforcement agencies. Most existing law enforcing systems were designed to address the fraudulent and

deceptive commercial practices against consumers when such practices were mostly of domestic nature. But after the growth of Internet it has been seen that current laws and systems are not capable enough to address cross border issues. A greater difficulty lies with respect to diverse legal systems, different laws worldwide and different law enforcement policies.

3.6 Definition of Jurisdiction and Why Jurisdiction is an Important Issue

The general meaning of the term jurisdiction refers to, 'Power of the State to exercise its authority over property and persons within its geographical limits'. However, in the context of dispute resolution, a clear concept of jurisdiction is needed to answer questions such as 'which is the most appropriate court to hear the dispute? What law will be applied to resolve the dispute? Which authority will enforce the judgment? In such circumstances the term jurisdiction would involve- 'The scope of the courts power to examine and determine the acts, interpret and apply laws, make orders and declare judgments. Geographic area, the type of parties who appear, the type of relief that can be sought, and the point to be decided may limit jurisdiction.'

The whole notion of jurisdiction is vital in the context of dispute resolution because of the deeply rooted relationship between physical proximity and the effects of any legal activity. Jurisdiction enables the States to monitor and control the activities of property and persons within and across its territorial boundaries. The subjects of a sovereign States laws are primarily located within its physical borders and so are greatly affected by the application of its laws. Legal theories about sovereignty, territoriality and an entity's physical presence support the traditional notion of a Courts jurisdiction in its role as adjudicator. These schools of thought recognize the sovereign power of a State and the territorial origin and application of a set of laws. A key assumption in all these theories is that a State, which is supported by the people of a particular area, makes laws which will only be valid, applicable and enforceable within its territory.

Cyberspace, which constitutes a technology-driven imaginary space, defies control by mechanisms evolved in the real world essentially based on geopolitical boundaries. It is a new social order, which cuts across cultures, civilizations, religions, etc. and creates a ''new realm of human activity'' forcing mankind to rethink the appropriateness of extending the existing rules to it. Cyberspace clearly disregards the general correspondence, existing in the

real world, between physical borders and 'law space''—based on considerations of power, effects, legitimacy and notice.

The law, in the ''non-virtual world'', works essentially on a two way premise that a certain set of legal rules is applicable to only one set of persons, who are present within the limits of the sovereign prescribing such rules, and to none other; and that a certain set of persons are required to comply with only one set of standards, and with none other. It is this perception, which having been mutually recognized and accepted by most sovereigns gives the requisite strength and legitimacy to each sovereign to enforce its legal rules within its territory. However, the case with the cyber world is different as it admits of no territory or polity based borders sufficient to impose a certain set of rules to a certain territorially defined set of persons. This leads each cyber actor to act according to his own legal order (or perhaps no legal order at all), leading to blatant violations of what may be guaranteed rights under other legal regimes. Litigation involving the internet has thus increased as the internet has developed and expanded.

Position in United States

A court does not have power over every person in the world. Before a court may decide a case, the court must determine whether it has "personal jurisdiction" over the parties. A plaintiff may not sue a defendant in a jurisdiction foreign to the defendant, unless that defendant has established some relationship with that forum that would lead him to reasonably anticipate being sued there. In the U.S., the Due Process clause of the Constitution's Fourteenth Amendment sets the outermost limits of personal jurisdiction.

There broadly two bases for a US court to exercise jurisdiction. They are: Firstly, Territoriality and secondly Jurisdiction over out of state defendant. Needlessly, physical presence of the defendant has always been a basis for personal jurisdiction. This is permitted over people who are within the territorial borders. Here, physical presence shall play the determining role, even when an out-of-state individual enters the forum state for a brief time. In case of out-of-state defendant who is not physical present, a US court requires to satisfy two broad principles, firstly, there must be authority with the court to try the case (i.e court must have jurisdiction) and secondly, due process clause of the Constitution must be satisfied.

If a party has substantial systematic and continuous contacts with the forum, a court may exercise jurisdiction over a party for any dispute, even one arising

out of conduct unrelated to the forum. This is known as general jurisdiction. For example, a corporation or person can always be sued in its state of residence or citizenship or its principal place of business, regardless of whether or not the claim arose there. If a party is not present in the state or does not have systematic and continuous contacts with the state, courts may exercise jurisdiction over a party for causes of action arising out of his contacts with the state, or arising out of activities taking place outside the state expressly intended to cause an effect within the state. This "effects" test is described from the American

Law Institute's Restatement (Second) of Conflict of Laws 37 (1971), which provides: "A state has power to exercise judicial jurisdiction over an individual who causes effects in the state by an act done elsewhere with respect to any cause of action arising from these effects unless the nature of the effects and of the individual's relationship to the state make the exercise of such jurisdiction unreasonable." To do this, the court must look to the state's "long-arm" statute, which sets the parameters for the state's exercise of its constitutional power to govern conduct by non-citizens (including both Americans and foreigners). Long-arm statutes vary widely from state to state. In order to be subject to personal jurisdiction in a state that is not his domicile, not only

must a person fit under the ambit of the state's "long-arm" statute, but also the state's jurisdiction must be valid under the Due Process Clause of the Fourteenth Amendment. The Supreme Court set the standard for constitutional exercise of jurisdiction in International Shoe Co. v. Washington. Pursuant to the Due Process Clause, a nonresident defendant may not be sued in a forum unless it has first established sufficient "minimum contacts with [the forum] such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." In addition, the nonresident's "conduct and connection with the forum such that he should reasonably anticipate being hailed into court there."

This test relies on courts to decide, according to "traditional notions of fair play and substantial justice," what contacts are sufficient. Courts will generally hold that contacts are sufficient to satisfy due process only if the nonresident "purposefully availed" itself of the benefits of being present in, or doing business in, the forum. According to a the plurality of the Supreme Court in Asahi Metal Industry v. Superior Court, a connection sufficient for minimum contacts may arise through an action of the defendant purposefully directed

toward the forum State. The placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State, but advertising or marketing in the forum state may fulfill the deliberate availment requirement. There must be clear evidence that the defendant sought to serve the particular market. If the minimum contacts test is met, a court may only exercise jurisdiction if it is "reasonable" to do so. In determining reasonableness, a court must weigh and consider the burden on the defendant to litigate in the forum, the forum state's interests in the matter, the interest of the plaintiff in obtaining relief, efficiency in resolving the conflict in the forum, and the interests of several states in furthering certain fundamental social policies.

In sum, under U.S. law if it is reasonable to do so, a court in one state will exercise jurisdiction over a party in another state or country whose conduct has substantial effects in the state and whose conduct constitutes sufficient contacts with the state to satisfy due process. Because this jurisdictional test is ambiguous, courts in every state of the U.S. may be able to exercise jurisdiction over parties anywhere in the world, based solely on Internet contacts with the state.

Jurisdiction from Indian Perspective

Effective legal machinery can be identified on how properly rules and regulations are drafted by legislators and more importantly how precisely principles of jurisdiction are laid down. A court must have jurisdiction, venue, and appropriate service of process in order to hear a case and render an effective judgment.

In India Jurisdiction of civil courts is divided into three categories: 1). Pecuniary, 2). Subject matter, and 3). Territorial

The term pecuniary jurisdiction means jurisdiction that is based upon monetary limits. Here the jurisdiction of civil court to deal with suits is dependent on the total value of the suit. It is the value of the suit it would be decided as to which court would be competent to deal with the case. For example, if the claim is below Rs. 1, 00,000, then the appropriate court would be Civil Judge (Junior Division). But if it is more than Rs. 1,00,000, then the appropriate court shall be the Civil Judge (Senior Division).

There can be instances when jurisdiction for certain subject has been exclusively vested in a particular court. In such case it is termed as subject

matter jurisdiction. For e.g. a petition for winding up of a company can be filed only in the concerned High Court.

Disputes between the parties relating to immovable property, arising through the Internet or otherwise, do not present any difficulty as to the jurisdiction of the civil court to entertain and resolve the suit which as discussed above depends upon the location of the immovable property, subject to one exception as stated above.

According to Section 19 of CPC, which deals with, compensation for wrong done to a person or to a movables, then in such case if the wrong was done within the jurisdiction of one court and the defendant resides, or carries on business or personally works for gain, within the jurisdiction of another court, a suit can be filed at the option of the plaintiff, in either of the courts having jurisdiction over the said places. Since plaintiff is the aggrieved party who files the suit, the law gives him the option to choose the place of suing from the stipulated alternatives wherever provided in law. On the other hand, since the defendant would have to defend himself, jurisdiction based on residence and works are to his convenience.

International and Municipal Jurisdiction the fact that international organizations, courts and tribunals have been created raises the difficult question of how to co-ordinate their activities with those of national courts. If the two sets of bodies do not have concurrent jurisdiction but, as in the case of the International Criminal Court (ICC), the relationship is expressly based on the principle of complementarily, i.e. the international court is subsidiary or complementary to national courts, the difficulty is avoided. But if the jurisdiction claimed is concurrent, or as in the case of International Criminal Tribunal for the former Yugoslavia (ICTY), the international tribunal is to prevail over national courts, the problems are more difficult to resolve politically. The idea of universal jurisdiction is fundamental to the operation of global organizations such as the United Nations and the International Court of Justice (ICJ), which jointly assert the benefit of maintaining legal entities with jurisdiction over a wide range of matters of significance to states (the ICJ should not be confused with the ICC and this version of "universal jurisdiction" is not the same as that enacted in the War Crimes Law (Belgium) which is an assertion of extraterritorial jurisdiction that will fail to gain implementation in any other state under the standard provisions of public policy). Under Article 34 Statute of the ICJ only states may be parties in cases before the Court and,

under Article 36, the jurisdiction comprises all cases which the parties refer to it and all matters specially provided for in the Charter of the United Nations or in treaties and conventions in force. But, to invoke the jurisdiction in any given case, all the parties have to accept the prospective judgment as binding. This reduces the risk of wasting the Court's time. Despite the safeguards built into the constitutions of most of these organizations, courts and tribunals, the concept of universal jurisdiction is controversial among those states which prefer unilateral to multilateral solutions through the use of executive or military authority, sometimes described as real politik-based diplomacy.

Do viruses and all the other nastiest in cyberspace matter? Do they really do much harm? Imagine that no one has updated your anti-virus software for a few months. When they do, you find that your accounts spreadsheets are infected with a new virus that changes figures at random. Naturally you keep backups. But you might have been backing up infected files for months. How do you know which figures to trust? Now imagine that a new email virus has been released. Your company is receiving so many emails that you decide to shut down your email gateway altogether and miss an urgent order from a big customer. Imagine that a friend emails you some files he found on the Internet. You open them and trigger a virus that mails confidential documents to everyone in your address book including your competitors. Finally, imagine that you accidentally send another company, a report that carries a virus. Will they feel safe to do business with you again? Today new viruses sweep the planet in hours and virus scares are major news. A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses can have harmful side effects. These can range from displaying irritating messages to deleting all the files on your computer. A virus program has to be run before it can infect your computer. Viruses have ways of making sure that this happens. They can attach themselves to other programs or hide in code that is run automatically when you open certain types of files. The virus can copy itself to other files or disks and make changes on your computer. Virus side effects, often called the payload, are the aspect of most interest to users. Password-protecting the documents on a particular day, mailing information about the user and machine to an address somewhere are some of the harmful side effects of viruses. Various kinds of viruses include macro virus, parasitic or file virus, Boot virus, E-mails are the biggest source of viruses. Usually they come as attachments with emails. The Internet caused the spreading of viruses around the globe. The

threat level depends on the particular code used in the WebPages and the security measures taken by service providers and by you. One solution to prevent the viruses is anti-virus software's. Anti-virus software can detect viruses, prevent access to infected files and often eliminate the infection. Computer viruses are starting to affect mobile phones too. The virus is rare and is unlikely to cause much damage. Anti-virus experts expect that as mobile phones become more sophisticated they will be targeted by virus writers. Some firms are already working on anti-virus software for mobile phones. VBS/Timo-A, Love Bug,Timofonica,CABIR,aka ACE-? and UNAVAILABLE are some of the viruses that affect the mobile phones

3.2 What is a Computer Virus?

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. Viruses normally have harmful effects. These can range from displaying irritating messages to deleting all the files on your computer.

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing securitysystems.

Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses.

Some people distinguish between general viruses and *worms*. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs[23].

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".[1][2][3][4]Viruses often perform some type of harmful activity on infected hosts, such as stealing hard

[23] http://www.webopedia.com/TERM/V/virus.html

diskspace or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Virus writers use social engineering and exploit detailed knowledge of security vulnerabilities to gain access to their hosts' computing resources. The vast majority of viruses target systems running Microsoft Windows,[5][6][7] employing a variety of mechanisms to infect new hosts,[8] and often using complex anti-detection/stealth strategies to evade antivirus software.[9][10][11][12] Motives for creating viruses can include seeking profit, desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore artificial lifeand evolutionary algorithms.[13]

Computer viruses currently cause billions of dollars' worth of economic damage each year,[14] due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and a multi-billion dollar industry of antivirus software vendors has cropped up, selling virus protection to users of various operating systems of which Windows is often the most victimized, partially due to its extreme popularity.[*citation needed*] No currently existing antivirus software is able to catch all computer viruses (especially new ones); computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.[15][24]

.

3.3 Evaluation of viruses in cyber space

In the mid-1980s Basit and Amjad Alvi of Lahore, Pakistan discovered that people were pirating their software. They responded by writing the first computer virus, a program that would put a copy of itself and a copyright message on any floppy disk copies their customers made. From these simple beginnings, an entire virus counterculture has emerged. Today new viruses sweep the planet in hours and virus scares are major news.

[24] https://en.wikipedia.org/wiki/Computer_virus

How does a virus infect computers?

A virus program has to be run before it can infect your computer. Viruses have ways of making sure that this happens. They can attach themselves to other programs or hide in code that is run automatically when you open certain types of files. You might receive an infected file on a disk, in an email attachment, or in a download from the internet. As soon as you launch the file, the virus code runs. Then the virus can copy itself to other files or disks and make changes on your computer.

Who writes viruses?

Virus writers don't gain in financial or career terms; they rarely achieve real fame; and, unlike hackers, they don't usually target particular victims, since viruses spread too indiscriminately. Virus writers tend to be male, under 25 and single. Viruses also give their writers powers in cyberspace that they could never hope to have in the real world.

Virus side effect

Virus side-effects are often called the payload. Viruses can disable our computer hardware, Can change the figures of an accounts spreadsheets at random, Adversely affects our email contacts and business domain, Can attack on web servers...

- Messages -WM97/Jerk displays the message 'I think (user's name) is a big stupid jerk!'
- Denying access -WM97/NightShade password-protects the current document on Friday 13th.
- Data theft- Troj/LoveLet-A emails information about the user and machine to an address in the Philippines.
- Corrupting data -XM/Compatable makes changes to the data in Excel spreadsheets.
- Deleting data -Michelangelo overwrites parts of the hard disk on March 6th.
- Disabling Hardware -CIH or Chernobyl (W95/CIH-10xx)
- attempts to overwrite the BIOS on April 26th, making the machine unusable.
- Crashing servers-Melissa or Explore Zip, which spread via email, can generate so much mail that servers crash.

There is a threat to confidentiality too. *Melissa* can forward documents, which may contain sensitive information, to anyone in your address book. Viruses can seriously damage your credibility. If you send infected documents to customers, they may refuse to do business with you or demand compensation. Sometimes you risk embarrassment as well as a damaged business reputation. WM/Polypost, for example, places copies of your documents in your name on alt.sex usenet newsgroups

3.4Influence of virus Attack on economically and Personal Cases

OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED*

A news- MUMBAI, 20 September 2007 — IT experts were trying yesterday to restore the official website of the government of Maharashtra, which was hacked in the early hours of Tuesday.

Rakesh Maria, joint commissioner of police, said that the state's IT officials lodged a formal complaint with the Cyber Crime Branch police on Tuesday. He added that the hackers would be tracked down. Yesterday the website, http://www.maharashtragovernment.in, remained blocked.

Deputy Chief Minister and Home Minister R.R. Patil confirmed that the Maharashtra government website had been hacked. He added that the state government would seek the help of IT and the Cyber Crime Branch to investigate the hacking.

"We have taken a serious view of this hacking, and if need be the government would even go further and seek the help of private IT experts. Discussions are in progress between the officials of the IT Department and experts," Patil added.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT experts working on restoring the website told Arab News that they fear that the hackers may have destroyed all of the website's contents.

According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as "Hackers Cool Al-Jazeera" and

claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail.

According to a senior official from the state government's IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.[25]

Duqu Trojan found in Indian Server**30/10/2011, 03:44:00 AM

Duqu Trojan found in Indian Server Last week we update you about Duqu when Symantec said it had found a mysterious computer virus that contained code similar to Stuxnet, a piece of malware believed to have wreaked havoc on Iran's nuclear program. Two workers at a web-hosting company called Web Werks told Reuters that officials from India's Department of Information Technology last week took several hard drives and other components from a server that security firm Symantec Corp told them was communicating...

[26]*Stuxnet's Son "Duqu" Removal Tool released by Bitdefender 21/10/2011 04:57:00 AM

[27]**Most advanced and dangerous malware for Apple products - why you should be concerned !** 28/10/2011 08:44:00 AM

Most advanced and dangerous malware for Apple products - Why you should be concerned ! Indian security researcher from MalCon has created an advanced and dangerous malware for Apple products which can not only compromise your privacy but also steal important data and let hackers control your device by simple text messages. If you are using any Apple product such as iPhone, iPad or iPod, then you should be concerned. Indian security researcher from MalCon, Atul Alex has created an advanced malware...

3.5Cell phones crime as a techno-legal perspective

Mobile phones have become essential tools for communication and information exchange in the last two decades. Many people rely on their mobile phones in their personal lives as well as their businesses. Most mobile phone users exchange very sensitive and private information using their mobile phones

[25] *http://www.cyberlawsindia.net/cases.html

**http://thehackernews.com/2011/10/duqu-trojan-found-in-indian-server.html

[26] * http://thehackernews.com/2011/10/stuxnets-son-duqu-removal-tool-released.html

[27] ~ http://thehackernews.com/2011/10/most-advanced-and-dangerous-malware-for.html

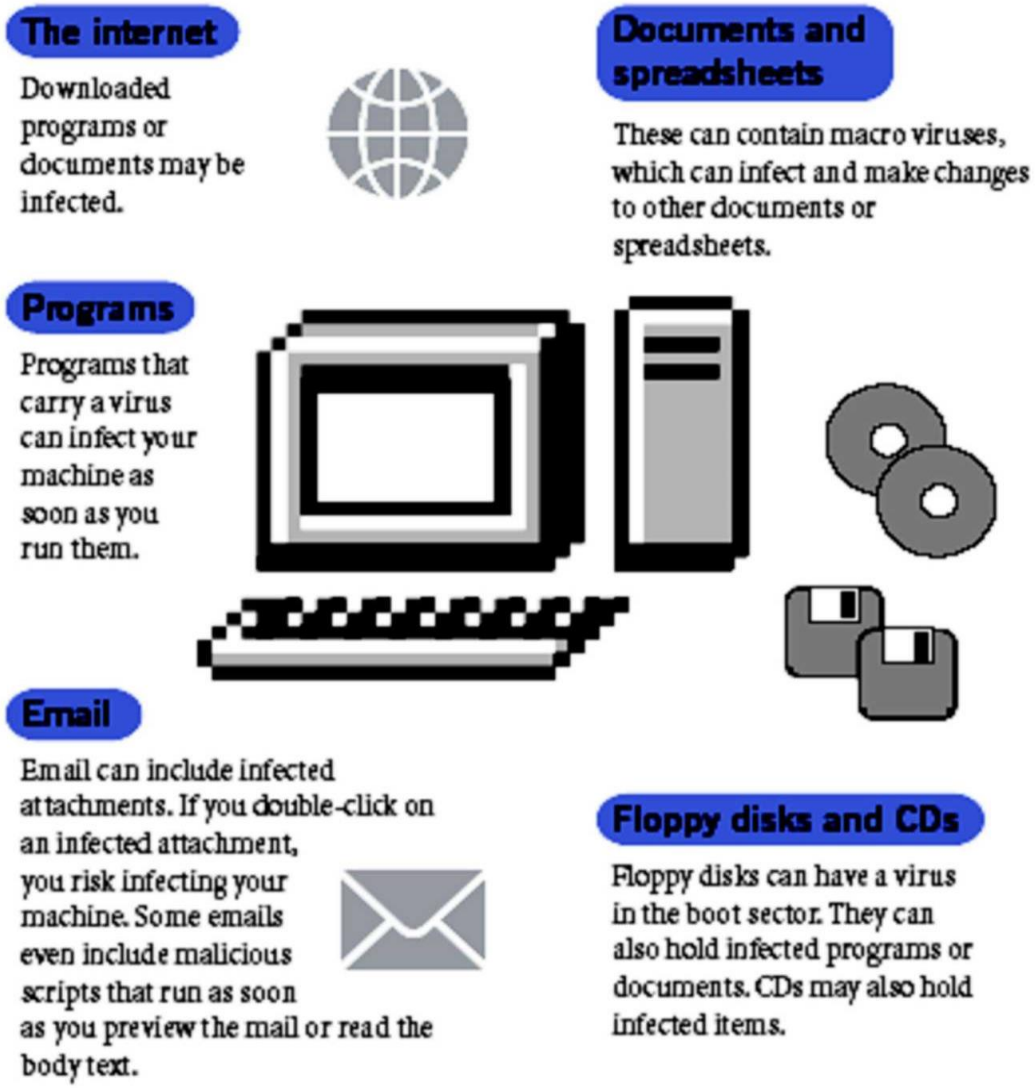
Main reference www.seminareproject.com

assuming that the mobile phone network is reliable and secure. These two incidents are examples to indicate that the privacy of the information and messages users send/receive by their mobile phones, can be legally or illegally breached by law enforcement officers, operators, or even other individuals or groups who have the technical expertise and the required equipment. What is even worse is that most users of mobile communication systems are unaware of or unable to deal with the many threats to their privacy. Recent statistics show that there are more than 21 million mobile phone users in Canada and this number is expected to reach 20 million by 2010 Mobile phone users in Canada (as many others worldwide) always assume that there is no reason to worry about the privacy of their phone calls and text messages sent over their mobile phones. To the best of our knowledge, no previous study has investigated the privacy of mobile phone users in Canada. This study investigates the threats to mobile phone users' privacy in Canada from technical and legal perspectives. We also propose a set of measures and recommendations to deal with these threats to improve mobile phone users' privacy.

Mobile phone systems are hybrid (wireless/wire lined) communication systems. As shown in the connection between the mobile phone and the serving unit called

base station uses wireless communication. On the other hand, base stations are connected to a sophisticated switching center (called mobile switching center) through optical fibers or microwave links. The connection between the base station and the mobile switching center might be direct or through a controlling unit called

base station controller. The mobile switching center connects the mobile phones to other mobile phones or to fixed phones through the public phone



network. The connections between the base stations, base station controllers, the mobile switching center, and the public switching telephone network usually use optical fiber or microwave links. The connections between the mobile phones and the base stations constitute the radio access network, while the connections between the base station and the mobile switching centers and between the mobile switching centers to each other and to the public switching telephone network constitute the core network also called the fixed network. A Simplified Model for the Mobile Phone Network Architecture. Mobile Switching Center Base Station

3.6 Threats and Risks to the Privacy of Mobile Phone Users

This chapter is a comprehensive yet interesting treatise on the existent and imminent threats facing the mobile phone users. These threats can be broadly categorized into two, namely; signal interception and access to user information. Access to user information can be subdivided into access to text messages, access to user records and access to stored information on mobile phone sets. These four threats are the germs upon which the first four sections of this chapter were developed. The first section commences by highlighting the background concepts underlying signal interception. This is followed with a proper definition for signal interception with special emphasis on the possible regions in the mobile phone network where signals can be intercepted. Afterwards, the reader is made to be aware of the some hardware and software techniques that can accomplish the task of signal interception. Upon discussing this, a critical review of analog mobile phone system is done and at the same time, analysis of the contemporary digital mobile phone system is done to reveal its vulnerabilities. This section ends with the discussion of pertinent cases to substantiate the claims made earlier in this section. The second section begins with a systematic introduction of text messaging to the meaning of access to text messages. Afterwards, this section points to the fact that law enforcement agents have access to text messages. After discussing this point, instances were cited to buttress this claim. Subsequently, the threats from malicious attackers were also brought into view with cases to validate the existence of such threats. This section ends with the mention of the combination of software and/or hardware tools for data recovery. The third section starts with a coherent description of what user records are and where they can be found. This is followed with the discussion of the various ways by which user records can be accessed from the mobile phone or the operator's database server. This section ends with citing of relevant cases to reinforce the explanations made earlier in this section. The fourth section commences the description of modern mobile phones and how they competently perform the role of data processing, storage and transmission. Subsequently, the different scenarios by which stored information can be accessed is brought to the reader's attention. This section ends with convincing real life instances to support the explications made earlier in this section. The fifth section is an exploration of other possible threats. The first issue to be looked upon is the possibility of using a mobile phone for tracking and locating a person. This was adequately supported with a news report. The other issue that was investigated in this section is the possibility of malicious threats to mobile phone users as a

result of Bluetooth technology. This was also sufficiently reinforced with a news report touching every nook and cranny of the issue. This section is concluded by a call for pragmatic and reliable mobile security solutions.

Signal Interception

Before delving into the details of signal interception, it is of utmost importance to trace its root back to its ancestor – eavesdropping. Eavesdropping is simply the act of secretly listening to a private conversation which can be viewed as either unethical or advantageous depending on the parties involved in this act and the underlying motives for indulging in such act. It can be done over telephone lines (phone tapping), email, instant messaging, and other modes of communication considered private It must be highlighted at this juncture that signal interception technically falls under phone tapping. Consequently, a brief explanation of what phone tapping is will undoubtedly shed more light on what signal interception really is. Phone tapping is the monitoring of telephone and internet conversations by covert means with the aim of gaining knowledge about the transmitted information and/or altering this information Hence, in this context, signal interception can be simply described as the acquisition and/or interruption of data which is being transmitted on the radio access network which represents the connections between the mobile devices and the base stations or on the core network which constitutes the connections between the base station and the mobile switching centers and between the mobile switching centers to each other and to the public switching telephone Network.

3.7 About MCA21

MCA21 project is designed to fully automate all processes related to the proactive enforcement and compliance of the legal requirements under the Companies Act, 1956. This will help the business community to meet their statutory obligations. The major components involved in this comprehensive e-Governance project are Front Office and Back Office. From the customer perspective, the Front Office operations assume significance, which would be administered through the Front Office portal. The entire Back Office operations of the MCA would be automated so as to achieve the objective of a user-friendly computerized environment. MCA portal is the single point of contact

for all MCA related services, which can be easily accessed over the Internet by all users.

The project also envisages a cost-effective integrated software solution for computerizing various in-house functions like Human Resources Management, Payroll, Accounting and Finance for internal users (employees) of MCA.

Adopting international best practices, MCA21 application adds immense value to the stakeholders. The following points highlight the project's invaluable importance:

- Enable the business community to register a company and file statutory documents quickly and easily.
- Public will get easy access to relevant records and get their grievances redressed effectively.
- Professionals will be able to offer efficient services to their client companies.
- Financial institutions will find registration and verification of charges easy.
- MCA will ensure proactive and effective compliance with relevant laws and corporate governance.
- Employees will be enabled to deliver best of breed services.

.

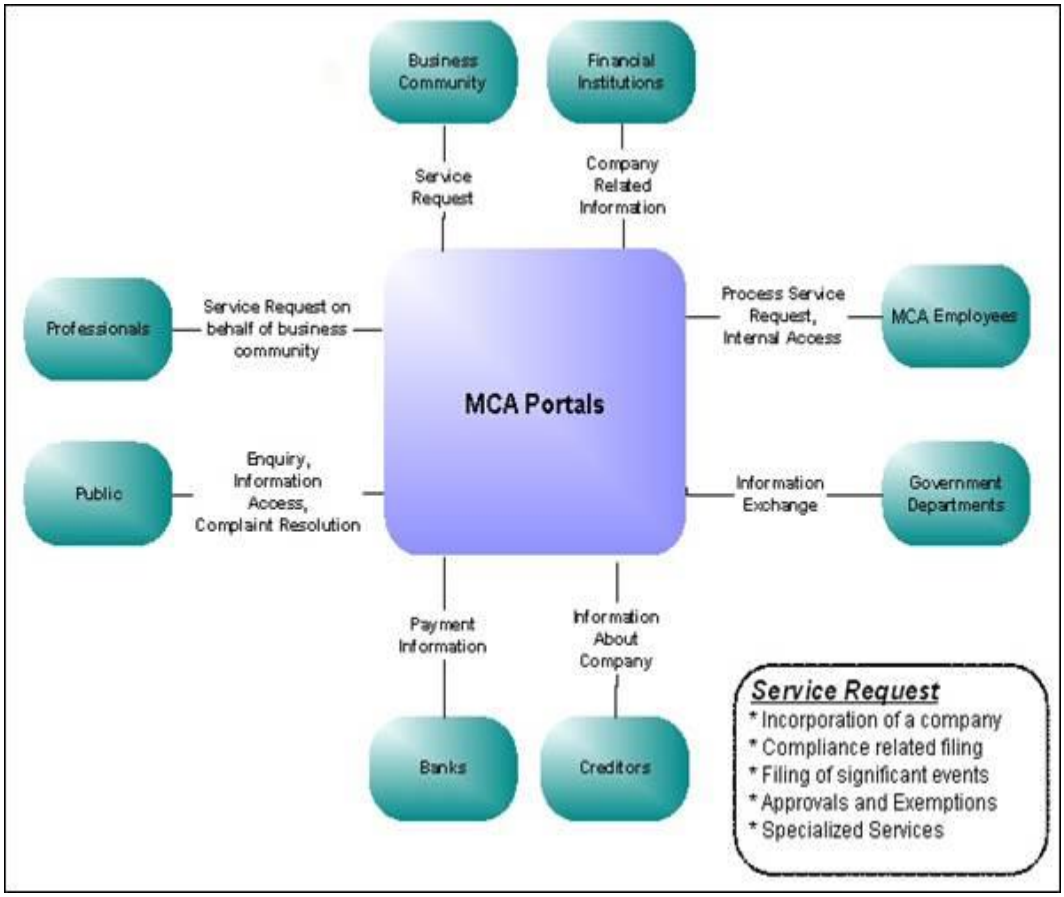


Figure 1: Context Diagram of MCA Portal

The re-engineered electronic forms, also called e-Forms, are capable of helping the citizens in the process of filling the information electronically. Lifecycle of e-Forms, the key interface to most MCA transactions, is automated from submission to the delivery of services requested therein. It covers dissemination of e-Forms in a reliable manner, efficient filling of information by eliminating re-entering data submitted in the past, electronic payment for and delivery of services as requested in the e-Forms. The business community can also track the status of their e-filing online.

The capability to automate the e-Form processing has also been extended to the Back Offices to meet the service levels committed to the business community. The e-Forms and attached documents, all in electronic format, are automatically assigned to the MCA staff and the progress tracked until the service is delivered to the citizens.

Besides e-Form service delivery to the business community, the MCA system includes tools for the analysis of corporate data for proactive surveillance and prosecution resulting in efficient investor protection.

3.8 What about spam techniques in cyber space

The Spam Act refers to spam as "unsolicited commercial electronic messaging".

"Electronic messaging" covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone. To be covered by the Spam Act, the message must be commercial in nature – for instance offering a commercial transaction, or directing the recipient to a location where a commercial transaction can take place. There are a large number of *commercial electronic messages* that can be sent legitimately. They are only considered to be spam if they are sent without the prior consent of the recipient – as unsolicited messages. A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

The Spam Act makes no reference to bulk messaging - a single unsolicited commercial electronic message could be spam.

PURPOSE OF THE SPAM ACT 2003

The Spam Act was developed in response to the problems caused by the growing volume of *unsolicited commercial electronic messages*, or spam. Spam threatens the viability and efficiency of electronic messaging. It damages consumer confidence, obstructs legitimate business activities and imposes many costs on users. The legislation prohibits *unsolicited commercial electronic messages*. There are, however, many legitimate uses for electronic messaging – it is an important tool for business. It allows simple and low cost communication with consumers who are increasingly using such technologies to access information. The Spam Act includes rules aimed at preserving legitimate business communication activities and encouraging the responsible use of electronic messaging. The Act says that *commercial electronic messages* must accurately identify their sender, and include a way for the recipient to *unsubscribe* from future such messages if they want to.

3.9 Crimes in spam?

Receiving spam is a common complaint of many Internet users. In fact, spam email has become an increasingly bothersome problem as individuals spreading spam email find easier ways to invade users' email accounts, leading to the necessity of such tools as spam filters and spam blocker features. Spam is a

huge issue for most Internet users – in fact, 52% of participants polled in a recent survey stated that spam was a major problem. And despite the evolution of anti spam software, such as spam filters and spam blockers, the negative effects of spam are still being felt by individuals and businesses alike. Think you know all you need to know about spam? Read on for some alarming spam statistics and facts about spam email. The UK has made spam a criminal offence to try to stop the flood of unsolicited messages.

Under the new law, spammers could be fined £5,000 in a magistrate's court or an unlimited penalty from a jury.

But they would not be sent to jail, according to the new measures introduced by Communications Minister Stephen Timms.

Spam has become the bane of internet users, with junk messages making up more than half of all e-mails sent.

3.10 Spam Laws

Anti Spam Law The US Can-Spam Act is the most famous anti-spam legislation, but not the only one. Get all the details here and see how Can-Spam affects your affiliate marketing. Outside the US, check up on spam laws in the EU, UK, Australia, New Zealand, Asia and Canada.

3.11 Need for Cyber Law in cyber space[28]

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

9. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

10. 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.

11. 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.

12. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly

[28] Introduction to Indian Cyber Law by RohasNagpal, Asian School of Cyber Law; retrieved from http://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf

hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

13. 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.

14. 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.

15. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

16. 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.

3.12 Jurisprudence of Indian Cyber Law in cyber space[29]

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

[29] 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

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 16thDecember 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.

3.13 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.

3.14 Summary

It is of utmost important to decide the jurisdiction of the court in order to empower the court to deiced the disputes between the parties concerned. The jurisdiction is a nonspecific term that refers to the authoritative power of the court to decide upon the cases. The general principles that decide the jurisdiction power of the court is territory and subject matter. Both are equally important while deciding upon the power of the court to decide dispute. These principles has always stood the test of time in all cases were geographical borders was to be taken into consideration while deciding the power of the court to decide the dispute. But with the growth of the Internet these traditional principles of Jurisdiction has become inadequate and a question has been raised, as to which court shall have appropriate jurisdiction to decide upon the case in case of on-line crimes. Since cyberspace does not respect geographical boundaries the developing law of jurisdiction must address whether a particular event of cyber crimes has to be tried by the laws of the country where internet service provider is located, the country where the user is located or country where the server is located. With these preliminary presumptions an attempt is made to analyze the current hypothesis being used for determination of cyberspace jurisdiction. The rapid growth of e-commerce and the liability of netizen's make the task more difficult. Since there is lack of single principle for ascertaining the jurisdiction over offences committed in cyber space and the adoption of different laws by different countries makes the task of determining jurisdiction more difficult.

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.

3.15 References

1. A Survey of Cybercrime by Zhicheng Yang, retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime/

2. Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

3. India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both"- In Indian Legal Perspective, by Rajkumar Dubey, retrieved

from
http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both

4. Dr. G A Solanki, “Jurisdiction in Cyber Space: Where to File a Suit?”

5. Amit M. Sachdeva, “International Jurisdiction in Cyberspace: a Comparative Perspective”

6. Golak Prasad Sahoo, “Jurisdictional Jurisprudence and Cyberspace”

7. Mr. K. I. Pavan Kumar, “Cyber Prudence”

3.16 Check your progress

1. _____ is a kind of offence which is normally referred as hacking in the generic sense.
2. _____ are event dependent programs.
3. _____ is derived from the term hi jacking.
4. _____ 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.
5. The term _____ primarily describes any amateur computer programmer who discovered ways to make software run more efficiently.
6. _____ is the law that is established through the decisions of the courts and other officials.
7. Law cannot function in vacuum it seeks a definite _____ voluntarily abiding to it.
8. The general meaning of the term _____ refers to, ‘Power of the State to exercise its authority over property and persons within its geographical limits’.
9. In India Jurisdiction of civil courts is divided into three categories: 1). Pecuniary, 2). Subject matter, and 3). _____
10 Section _____ of the IT Act extends jurisdiction to any offence or contravention committed outside India by any person.

3.17 Answers to check your progress

1. Unauthorized access
2. Logic bombs
3 .Web jacking

4. Paedophiles

5. Hacker

6. Case law

7.Place and People

8. Jurisdiction

9. Territorial

10. 75

3.18 Terminal Questions

1. Discuss the character of cyber criminals.
2. What do you understand by conventional and cybercrime? Explain in detail.
3. Describe some cyber crimes viruses.
4. Explain spam Techniques'?
5. What do you understand by Jurisprudence?
6. Discuss the importance of jurisdiction issue in cyber law.
7. What do you understand by Cyber invasion?
8. Examine the provisions relating to jurisdiction under the Information Technology Act.

Unit-4
Construction of Electronic contract

OBJECTIVES:

After going through this unit you should be able to:

- Understanding the meaning of electronic contract and objectives behind it.
- Understanding the legal perspectives for electronic contract
- Understanding the phases of E contract with relevant case study.

Structure:

4.1 Introduction

UNDERSTANDING ELECTRONIC CONTRACTS

The Indian Law of Contract

To understand electronic contracts, it is essential to understand the general principles of contract and also the law governing contracts in Indian context. Contracts are in essence an agreement between two or more parties to conduct any business transaction. Such a contract has to be valid and legally binding on the parties to mutually benefit their interest and transactions. Such contract can be oral or written as may be required by law in specific cases and

is validated by the law. Before the evolution of the complex legal systems, agreements were oral and carried out by mutual trust. In community settings any breach of contract is settled through community adjudication system, which inquired into the breach and set right things. As the society grew complex and so were the complexities of the transactions. With the evolution of the legal system, contracts came to be governed by specific laws under the respective legal systems. It can be stated that 'a contract is a agreement for a specified transaction between two or more parties for a specified consideration and is binding upon on the transacting parties.' The Contract, which could be oral or written, is arrived through a process of negotiation with offers/proposals, counter offer/counter proposals towards acceptance by the contracting parties. Such an acceptance gives rise to an agreement. Indian Contracts Act 2(h) states that 'an agreement enforceable by law is a contract.'

A Contract enforceable by Law

The Indian Contract Act 1872-s10 states: S 10. What agreements are contracts: All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void. Nothing herein contained shall affect any law in force in India, and not hereby expressly repealed, by which any contract is required to be made in writing or in the presence of witnesses, or any law relating to the registration of documents. Interpreting the section 10 of the Act the positive aspects can be enlisted as:

1. Free and conscious consent of the parties to the contract:

In other words there should not be any coercion, undue influence, fraud, misrepresentation or mistake which will not be considered as free consent and will be considered as void.

2. Persons entering to the contract should be competent:

In other words persons who are minors by law, persons with unsound mind are not competent and any contract entered with them is non-enforceable.

3. Lawful Consideration:

In other words any contract which is violative of any other law or considerations which not legal will not be valid and will be void

4. Lawful Object:

The purpose of any such contract has to be lawful in its object or else will be rendered as void. S17 fraud S 18 misrepresentation S 20 mistake Void Voidable agreements S 19 – This section deals with the instance of an agreement which is concluded by coercion, fraud, or misrepresentation, the

contract does not become void automatically but can is voidable at the option of the party whose consent was caused by those listed in section 14- 20. To illustrate that A enters into an agreement with B to sell his business with misrepresenting the facts of profit and goodwill and later when B finds about the same, B has the choice to make the contract void or can still proceed with the contract for other extraneous reasons and thus the contract is not void but had the choice to be made voidable by B who choose not to do so.

Void Agreement

1. s 20 – Both parties are under mistake as to the matte of facts
2. s 24 Consideration and objects are unlawful in part
3. s 25 Absence of consideration, except under certain cases
4. s 26 The agreement in restraint of marriage
5. s. 27. The agreement in restraint of trade
6. s 28The agreement in restraint of legal proceedings
7. s 29The agreement in restraint of uncertainty
8. s 30Agreement based on wager/gambling
9. s 56Agreement becomes impossible to perform

Contingent Contract S31- 36- speaks about the type of contracts entered which has to be performed or not to be performed based on the eventuality of an event to happen or not to happen and is enforceable accordingly. However the contingent contract would be void if the event becomes impossible to happen.

Breach of Contract

Section 73 of the Act Speaks about the breach of contract and appropriate remedies. This section enforces the binding nature of the contract and its legal validity. This section enumerates the loss or damage occurred to one party by the breach of contract of the other party, which is due to such breach of contract or prior knowledge of such consequence when the contract was entered to be compensated by the party who has breached it. In such calculation of loss or damage, the means of such consequence resulting from the non-performance of such contract has to be taken into account.

CONSTRUCTION OF ELECTRONIC CONTRACTS

Contracts in the traditional information technology prior to the Internet age pertained to :

1. Manufacturing contracts of hardware products, accessories and peripherals
2. Contracts for software products
3. Contracts for service and maintenance and post- online era brought in the
4. Electronic Contracts or Online contracts

With the emergence of internet and electronic commerce the contract of e-commerce in terms of Business to Business (B to B), Business to Consumer (B to C) and Consumer to Consumer (C to C) has assumed importance in terms of its complexity and reach. Electronic Banking, .Com ventures, Music download, E-books have spanned the usage of Internet and online -contracts have assumed significance. Among these contracts the manufacturing contract of hardware is that of any other type of contract in manufacturing industry except that of the latest issue of monopoly or anti-trust where browsing software is bundled with that of the hardware to keep up the market share which shall be dealt latter. On the software contracts the contracts assumed significance based on the type of software as

a. Standard package software
b. Bespoke software and
c. Customized software

The standard software is the type of software written and produced to address mass consumers around the world. Microsoft Windows and its different versions fall under this category. Bespoke software is the type of software specially commissioned and written to meet the needs of specific needs of varied clients. Many Indian software firms are involved in bespoke software production. E.g. an airline company may want bespoke software, which will suit its operations. Infosys in the early nineties did software for retailing Reebok shoes. Customized software is a standard software package, which is altered to the needs of the clients.

Many hospital and hotel administration software packages are standard software packages often modified to meet the variations of the customers. There are many networking packages, which are tinkered and tailored to meet client specific needs.

The contract of these software are dealt as manufacturing contracts where hardware manufacturers can bundle as standard software packages and the others like customized and bespoke software are dealt as contracts between parties based on the functionalities and thereby the terms of the contract. It is in this area care has to be taken in construction of contracts which will include

offshore and on-site issues involved in developing such packages. On-site contracts need to take into account of not merely the technical aspects and delivery of the software but also labour laws, gender laws and other accounting aspects of the country where the firm intends to operate in drawing up the contracts. Electronic Contracts Electronic contracts facilitate transactions and agreements electronically without the parties meeting each other. This means that the traditional contract process of offer, acceptance and agreement to transact through electronic mode than physical mode of paper. E-Commerce to succeed such contracts need to be validated legally an alternate mode of transaction through online using the latest technological developments. This is aimed at:

4.2 Computer electronic contract

1. To create a secure atmosphere of transacting online with alternate mode to paper and writing.
2. To create a electronic documentation system which will safeguard the contracting parties on par with the traditional mode of contracts
3. To create statutory status and monitoring/verifying authorities for such electronic transaction
4. To check frauds intentional or unintentional transactions to promote and build confidence in genuine online transactions
5. To create necessary legal structures to oversee such transactions
6. To establish standard rules and regulation for smooth functioning of online transactions
7. To make Digital signature legally valid and incorporating the same with the existing legal regime of contracts, sale of goods, evidence and consumer acts. Such electronic transactions will depend on the appropriate legal framework, which recognizes 'electronic records' or 'writings' or 'digital signatures'. It should facilitate for a secure system of such transactions and should create evidentiary value of such records. The Indian IT Act 2000 section 2 deals with various definitions involved in internet transaction and Chapter II and section 3 deals with the definition of digital signature and its authentication for legal purposes.

Section 4 of the IT Act 2000 reads as follows: 4. Legal recognition of electronic records where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding

anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference

4.3 Objectives

If any information or matter is rendered or made available in an electronic form, and accessible so as to be usable for a subsequent reference shall be deemed to have satisfied the requirement of the law, which provides that information or any other matter shall be in writing or in the typewritten form.

Legal recognition of digital signatures. -

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation. - For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

If any information or any other matter is required by law to be authenticating by affixing the signature then such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of digital signature affixed in the prescribed manner. Thus with the IT Act 2000 the necessary legal validity for electronics has been established. In this context the earlier Indian Contract Act has bee supplemented with the online transaction as a valid form of contract. In electronic contracts the twin aspects of time and place of dispatch assumes importance between the contracting parties. Online contracts whether it is B to B or B to C will to be validated the place of the dispatch and time factors are crucial. IT Act by section 11. -

11. -Attribution of electronic records. -

An electronic record shall be attributed to the originator-

(a) If it was sent by the originator himself;

(b) By a person who had the authority to act on behalf of the originator in Respect of that electronic record; or

(c) By an information system programmed by or on behalf of the originator to Operate automatically.

12. - Acknowledgment of receipt. -

(1) Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by-

a. any communication by the addressee, automated or otherwise; or
b. any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

4.4 Legal scenario & Legal provisions

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent. In internet transactions the time and place of dispatch and receipt of electronic records will play a crucial role in the aspects of territorial jurisdiction, applicable laws, evidentiary issues, period of limitation on initiation of litigations and other issues. To validate such contracts, section 13 of the IT Act has enabling provisions. S 13. - Time and place of dispatch and receipt of electronic record. -

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely: -

(a) If the addressee has designated a computer resource for the purpose of receiving electronic records, -

(i) Receipt occurs at the time when the electronic, record enters the designated computer resource; or

(ii) If the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section, -

(a) If the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "Usual place of residence", in relation to a body corporate, means the place where it is registered. Section 12 and 13 read together is the online equivalent to the traditional contract act transaction aspects of offer and acceptance.

Issues of Security : In electronic commerce the issue of security and a statutory monitoring agency become crucial factors and the same will become crucial aspects of electronic contracts for the consumers to protect their interests and for the business establishments to conduct their business without costly legal battles. The essential security aspects of e-commerce, which need to be taken care in contracts, Electronic 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 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.

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 facie 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. 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.

4.7 Cyber Forensic Tool

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.
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.

4.8 Case Laws

IN THE LABOUR COURT OF SOUTH AFRICA HELD AT DURBAN

CASE NO: D204/07

Reportable

Date Heard: 19-20 May 2008
Delivered:1 July 2008

In the matter between
S. B. JAFTA APPLICANT
and
EZEMVELO KZN WILDLIFE RESPONDENT

JUDGMENT

PILLAY D, J
Introduction

1. Does acceptance of an offer of employment sent by e-mail or short message service (SMS) result in a valid contract? When is an acceptance of an offer sent by e-mail or SMS received? Is an SMS an electronic communication? What is an electronic communication? To answer these electronic commerce or e-commerce questions that arise in this claim for contractual damages, the court looks to the Electronic Communications Transactions Act No 25 of 2002 (ECT Act). As the ECT Act has its origins in international law, the court also looks to international and foreign law for best practice.

4.9 Misuse of electronic contract

Computer contract 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 organizations now look to the experts to uncover this evidence discreetly and without disrupting business continuity.

4.10 Summary

Computers electronic contract 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.

4.11 References

1. An investigation of Computer Forensics by Ryan Pidanick; retrieved from http://www.isaca.org/Journal/Past-Issues/2004/Volume-3/Pages/An-Investigation-of-Computer-Forensics.aspx
2. Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf
3. Issues in Computer Forensics (.pdf) by Sonia Bui et. al; retrieved from http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf
4. Computer forensics (cyber forensics) by Margaret Rouse; retrieved from http://searchsecurity.techtarget.com/definition/computer-forensics
5. Plethora of Cyber Forensics by N. Sridhar, et. al.; retrieved from http://thesai.org/Downloads/Volume2No11/Paper%2018-%20Plethora%20of%20Cyber%20Forensics.pdf
6. The challenges facing computer forensics investigators in obtaining information form mobile devices for use in criminal investigations by David W. Bennett; retrieved from http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/
7. Cyber Forensics: law and practice in India | iPleaders http://blog.ipleaders.in/cyber-forensics-law-and-practice-in-india/#ixzz3FpZ7Gmxg
8. Electronic Evidence and Cyber Law by Adv. Prashant Mali; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a
9. Cyber Forensics in India; retrieved from http://perry4law.org/cfii/

4.12 Check your progress

1. The _____ is the process of identifying evidence material and its probable location.

2. The _____ saves the state of evidence that can be further analyzed.
3. The analysis phase collects the _____ and examines it to find the pieces of evidences.
4. The reporting phase comprises of _____ and _____ retention.
5. The main objective of _____ is to extract digital evidence which can be admissible in court of law.

4.13 Answers to check your progress

1. Identification phase
2. Acquisition phase
3. Acquired data
4. Documentation and evidence
5. Cyber forensics tools

4.14 Terminal questions

1. Explain the concept of cyber tools with example?
2. Discuss different phases of computer contract.
3. What are the objectives of e-contract?
4. Describe the forensics methodology in digital world.
5. What are the legal regulations mentioned in cyber forensics?

Unit-5
Types of Electronic contract

OBJECTIVES:

This Unit has been prepared to acquaint you with

- Various kinds of Contract. What is employment Contract? What is Consultant contract
- Software Development and Licensing agreement
- Misuse of Contract

Structure

TYPES OF ELECTRONIC CONTRACTS

5.1 Employment Contracts

The Information Technology is driven by manpower in Indian context and thus employment contracts are crucial. With a high attrition rate as well as the confidentiality involved in the work employment contracts become crucial. Apart from that Indian Labour practices are based on strong labour laws and not the hire and fire processes of the first world. In this context copyright issues of software development assumes crucial importance. This is dealt in

detail in module II but however due care should be taken on the aspect of restraint of trade which could be void in any contract. Apart from that contracts for on-site development and sending the workforce abroad and indemnity clauses will play a crucial role in employment contracts. Firms hiring personnel abroad apart from their personnel need to incorporate the relevant employment contract of the place of operation.

5.2 Consultant Contracts

The normal provisions of Indian Contracts Act of 1872 will apply on any consultant agreement. But especially in Information Technology industry where the infrastructure to operate is low and connectivity is very high consultancy with experience marketing and business development and technology development is a very prevalent mode of transaction. Here proper care to be taken in Consultant agreements where issues of Intellectual Property Rights, Confidentiality will play a key role. If care is not taken it may lead to loss of business and loss of clients.

5.3 Contractor Agreements

As manufacturing companies outsource their business, Information Technology also outsource their work due to fluctuating orders and would like to cut on the cost of regular workforce and attendant legal and financial problems. At the same time in manufacturing industry strong labour laws like the Contract Labour (Abolition and Regulation) Act of 1970 in force could lead to a different type of legal tangle. However if care is taken to outsource keeping the provisions of the contract Act and the Contract Labour abolition act the desired objectives could be met. Here again confidentiality, consumer liability and copy right issues assume great importance and care to be taken in drawing such contracts.

5.4 Sales, Re-Seller and Distributor Agreements

In software and Internet transactions though the hierarchy of middle men are done away with, it still requires a distribution network and hence contractual issues come into play in that aspect of business. In first place one needs to see whether software is a good under the Sale of Goods Act. Software is a code of instructions, which operate the system or hardware to function in an intended manner. Hence there arises a difficulty to classify and define in

legal terms of the intangible nature of software in comparison with other products. The code and its source can be interpreted as information organized in a way to operate the system leading to the conclusion it is not a property and not a good in the legal sense. In Aerodynamics Systems Product v General Automation limited, the argument raised by the defendants that although software can be a subject matter of sale, software itself is pure information, and the transfer of software is a service and not sale of goods. There is another interpretation of Software to be considered as Goods where it is compared to that of a book containing information, which is considered as goods under the Sale of Goods Act. As the value of the book is not the mere value of the cove jacket, paper and materials used in its production, but one that of the value of the information contained in it, software is also a product –a floppy, or a CD-Rom or simply stored in hard disc but the value is much higher than the simple storage device Hence software due its high value in terms of application is considered as goods for the purpose of legal classification. Having established it as good the distribution, reseller agreement should take care of the aspect of Monopoly Restrictive Trade Practices (in future the competition law) territorial jurisdiction and other tax mechanisms.

5.5 Non-Disclosure Agreements.

Non-Disclosure Agreements are part of IT contracts, which specify binding agreements with employees apart from the standard confidentiality agreements. The Indian Contract Act 1872 has provisions for the same and it assumes importance in an industry which is purely knowledge based and one which can be easily duplicated ruining the business.

5.6 Software Development and Licensing Agreements

A license is a permission given to do a specific manufacture/sales/marketing/distribution, which is lawful. License plays a prevalent form of contract in mass marketing activity of any kind including Information Technology. Software licensing has a historical background where originally it was bundled with the hardware and was given free and its use and application was limited to that of operating the system and few other features. Later in late 60's and early 70's hardware manufacturers in Europe marketed software separately. Later software manufacturers resorted to license their products separately from that of the hardware. In normal ownership the product sold becomes the exclusive property of the buyer who can do whatever he

wants. In case of software, the product can be copied easily and will adversely affect the manufacturer of his sale and thus the entire investment-return processes and future incentive to invest in producing software. Thus software business became a business of license regime. These licenses are issued in perpetuation or for a limited period. Licensing agreement normally prohibits reverse-engineering, de-compiling or any other manipulation of the software, which can be marketed easily with some modifications. Licenses are issued for a single machine usage at a specified location with a provision for backup in the same machine in case of a crash or defective functioning. Multiple machine licenses are also given. The license agreement also indemnifies the user from any copyright or other intellectual property violation of the manufacturer. The licensing agreements Become crucial in Cyber Contracts. Similarly software development is another agreement between joint ventures of companies or for awarding development of software to multiple parties, which assume crucial importance in contracts of cyber world.

5.7 Shrink Wrap Contracts

A Shrink Wrap contract is the prior license agreement enforced upon the buyer when he buys software. Before he or she tears the pack to use it, he or she is made aware by tearing the cover or the wrap that they are bound by the license agreement of the manufacture. This is done as earlier discussed to protect the interests of the manufacturer where the consumer cannot reproduce the package, copy it or sell it or donate it to others affecting the sale of the software. The license, which is shrunk and wrapped in the product, which becomes enforceable and taken as consent before the buyer tears the package. The usual clauses that are part of the shrink-wrap license are that of

a. prohibiting unauthorized creation of copies
b. prohibiting rentals of the software
c. prohibition of reverse engineering, de-compilation or modification
d. prohibition of usage in more than one computer specified for that purpose
e. disclaimer of warranties in respect of the product sold
f. limitations of liability

The logic and business sense is that to protect the manufacturer of the package, as it is easy to copy, manipulates and duplicate under other brand name. Critiques argue that shrink-wrap license agreement is against the basic principle of contract of offer, consideration and acceptance as the licensee is

debatable. Several cases to this effect have been dealt in US courts. A detailed analysis of the cases will be dealt in the website of nalsarpro.

5.8 SOURCE CODE ESCROW AGREEMENTS

In software development many principal firms who invest in development are keen to guard the source code of the software, which is the most valuable and secretive part of the computer programme. Copyright holders of such source code may have to disclose this to various developers who will be developing specified software based on the source code. In these circumstances the copyright owner will deposit the source code to specified source code escrow agents who will disclose the code on the development of the product upon agreed terms. In cyber contracts such agreements and also the terms and conditions to deal with the escrow agents becomes crucial.

5.9 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.

5.10 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.

5.11 References

1. Criminal Liability for misuse of information technology by Seth Associates (Advocates & Legal Consultants), retrieved from http://www.sethassociates.com/criminal-liability-for-misuse-of-information-technology.html
2. Offences and Penalties under the Information Technology Act, 2000 by Pradnya (November 17, 2010); retrieved from http://www.legalservicesindia.com/article/article/offences-&-penalties-under-the-it-act-2000-439-1.html

5.12 Check your progress

1. _____ is a full form of UNCITRAL Model Law.
2. Hacking with computer system described in _____ of IT, Act 2000.
3. Section 67 describes publishing of _____ in electronic form.
4. _____ able to direct a certifying authority or any employee of such authority for taking measures.
5. Penalty for misrepresentation is discussed in _____.

5.13 Answers to check your progress

1. United Nations Commissions on International Trade Law
2. Section 66
3. Obscene information
4. The controller
5. Section 71

5.14 Terminal 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.

Unit-6

Legal Issues in Cyber Contract

Objectives:

This unit has been prepared to acquaint you with

- Legal issues related with Cyber Contract
- How adjudication of those contract is done.

Structure

6.1 Introduction

CYBER CONTRACTS AND INDIAN LEGAL POSITION

Legal issues in Cyber Contracts:

The Intellectual Property Rights plays a crucial part in Information Technology and thereby in the contract formation of software development and Internet business. In Indian context software is categorized under copyrights of the IPR regime where as in United States software comes under patents regime. This difference has to be borne in mind in formation of contracts depending on domestic and international operations. Here again the IPR differs with the type of software classification. In case of bespoke software the intellectual property rights are vested in the software user. The copyright aspect is very crucial in the bespoke software compared to that of the confidential aspect of information.

Mere commissioning of a software development itself need not vest the copyright with a firm if the clauses in the contract are not specific. In U.K. the standard conditions of contract published by Government for information systems have provided for ownership of copyright and other rights in bespoke software to vest in the software house, and not in the government. Even if the ownership of the rights in the software vests in the software house, the customer's competitive edge can be preserved by imposing a restriction on the ability of the software house to market the software to the competition of the customer.

6.2 Contract liability

Contract liability is another crucial area to be taken care in cyber contracts. One of the general distinctions in contract liability is based on the classification of the utility of the software in transaction.

(a) License of Intellectual property.

(b) Development and / or supply of a copy of the software.

In the licensing aspect of the software the usual contractual risk arises in the third party possessing the Intellectual property rights which is overriding that of the rights of the licensee. The phrase software contracts connote a valid and a legally binding relationship created by the parties to enrich their interest. Parties to such software contracts generally include the consultant (a company or a partnership or a sole proprietor represented through business manager or technical manager or finance manager) and the customer who seeks software related services from the consultant company. The nature of the services may include sale of software products or software maintenance services either in the form of fixed priced project or time in maintenance.

6.3 Online Contracts

It is a common practice that transactions of many goods and services depend and use standard form of contract of terms and conditions, which are quite often hidden from the user or not prominently displayed. As the going is good there is no problem on such practices but in a business where the volume and risks are high such fine print or hidden terms may prove too costly when someone decides to act. Simply 'I agree' button displayed in front without reasonable and adequate display of the terms and conditions displayed to the buyer or user could lead to costly litigations in online transactions especially in B to C business. This necessitates effective and clear drafting of the terms of

contract where the drafting language has to be clear, transparent, to place across the business proposition or offer without jeopardizing the interest of the business where the language could lead to multiple interpretations and running the risk in a court battle. Such drafting requires the drafter to understand the fundamentals of

1. The relevant law in operation;
2. The practical implications of such law
3. The purpose and goal of the firm intends to achieve by such offer
4. How to use the relevant law and its implications to the maximum advantage
5. How to minimize the liability risks in unforeseen circumstances

DRAFTING OF CYBER CONTRACTS **

** (Extracted from nlsiu law shop series on software contracts-Jan 1999)

Description of the Parties In all but the shortest of documents it is obviously more convenient and clearer to refer to the various parties by such descriptive terms as vendor purchaser, guarantor, franchisee, etc. These terms are so basic to the agreement that they are invariably set out at the head of the document as part of the descriptions of its registered office or (particularly in the case of foreign companies which may not have a registered office) its principal place of business. Although it is not strictly

necessary to cite the company's registration number, it is sometimes useful to do this, as it may facilitate any search which has to be carried out and may avoid confusion where companies in a group with similar names are involved in the transaction. Language of the Agreement In International contracts particularly, specifying the language of the agreement can have a number of advantages, including:

(a) If the agreement has been drawn up in versions in different languages, it will be desirable to state which is the authoritative versions in different languages, it will be desirable to state which is the authoritative version, in the event of a difference in meaning between different versions.

(b) It may also be desirable to state that any amendments to the agreement should be in the same language as the original. In some jurisdictions the language of the agreement may influence the court when deciding under which country laws the agreement is made, and which country's courts should have jurisdiction. Ideally the agreement should state these matters specifically. Recitals After the description of the parties to a document come the recitals. Recitals in a document are synonymous to the preamble of a statute. The

recitals make out the state the preliminary ground or introduction for the execution of the Agreement. They constitute a brief history of the facts and events leading to the execution of the Agreement. Recital in a document means a statement in an agreement or other formal instrument introduced to explain or lead up to the operative part of the agreement. Recitals are of two types i.e. narrative and introductory.

Definitions and Interpretation

Particularly in long or complex agreements it is good practice to group all defined terms, together with their definitions, in a separate 'Definitions' clause, and to indicate elsewhere in the test of a document that a term has been so defined by starting the word or words defined with a capital letter. This will signal to anyone reading a clause in the body of the agreement that particular term has a special defined meaning in that agreement. It is essential using this method, for all defined terms to be capitalized on every occasion they are used, and that any term which is used in a wider sense than the one which is defined should not be capitalized. Whichever style is used, care must be taken when preparing a document to distinguish defined terms from terms of non - specific application. It is convenient to list the defined terms in alphabetical order, in a clear, easily assimilated layout. Where the meaning of a term will involve a lengthy description or list, the details can be assigned to a schedule or exhibit. In drafting practice, interpretation provisions are often combined with the definitions of terms used in the agreement under the heading Definitions and Interpretation'. The usual interpretation provisions deal with the following: Amendment/replacement of statutes; Persons/singular/plural: For the sake of brevity and to avoid any confusion; Reference to clauses: To ensure a clear economical style of drafting;

Headings

CONDITIONS AND ASSURANCES

(1) Commencement

Unless it is otherwise provided, an agreement takes effect immediately it has been signed by all parties or, in the case of an agreement executed as a deed, upon delivery of the deed. Sometimes parties will wish to provide for a different commencement date. This should be done by including a clause and not by misstating the date of the agreement (i.e. the date of the last signature) as this can amount to a forgery.

(2) Conditions precedent

Sometimes an agreement is stated not to come into effect until the happening of an event (this might refer, e.g., to finance being raised or government approvals being obtained or facilitating of base materials by the concerned contracting party. Such terms are known as conditions precedent. The clause does not need to use the phrase condition precedent' but the consequences of the condition not being met should be clearly stated. In particular, does the agreement as a whole automatically come to an end or do certain provisions continue? Is there a time limit for conditions to be met? All these details should be specified in the agreement to avoid confusion.

(3) Further action required after completion

In contracts of the single transaction type, in particular sale agreements, mortgages, intellectual property assignments and licenses etc., it is likely that after completion of the transaction further action will be required by one or both parties to perfect title or conform to statutory rules or in some other way to finish off the transaction satisfactorily. In order to avoid argument or delay in respect of such matters it is usual to provide exp of attorney must be expressly stated to be irrevocable. Force Majeure Where a contract becomes impossible to perform, or is capable of performance only in a manner substantially different from that originally envisaged, then in the absence of express provision by the parties further performance is excused under the common law doctrine of frustration. This doctrine only operates where the frustrating circumstances are not due to the fault of either party (See Denmark productions Ltd. v Boscobel Productions Ltd. (1969) QB 699 at 725. (1968) 3 All ER 513, 533 CA), but it does not follow that in all contracts any act of negligence will deprive a party of the defense of frustration. (See Joseph Constantine SS Line Ltd. v Imperial smelting Corn Ltd (1942) AC 154 at 166, 179,195, 205 (1941)) All ER 165 at0173, 182,193,199,200 HL) To avoid bringing the contract to an end under the law of frustration, a 'force majeure' clause is frequently incorporated into Indian law contracts, under which the parties expressly agree to exempt each other from performance of the contract or liability for breach of contract where the failure to perform is due to factors beyond that party's control. Thus where force majeure or an event of force majeure is deferred to in the agreement, it should be clearly defined.

Warranties and Indemnities / Guarantees Many commercial contracts contain warranties by one or both parties. These may include warranties as to matters which are central to due performance of the contracts but which cannot easily be verified by the other party. The exact nature of these warranties will

depend on the transaction being entered into. Whereas some types of warranties are specific to the individual transaction, others are found in many types of commercial agreement. Warranties as to a party's ability to enter into an agreement of the type in question, and as to the good standing of each party, are sometimes inserted in commercial agreement. In the longer type of agreement, it is frequent for the numerous detailed warranties to be given by, say, a vendor to be set out in a schedule to the agreement and for that party to give in the agreement an overall warranty as to the truth and accuracy of the scheduled warranties. A party giving warranties will commonly seek to limit the warranties to matters, which are within its knowledge.

An indemnity clause, often of a general and all embracing nature, is frequently included in agreements and contracts for services and the documents. Such a clause, whereby one party undertakes a separate and independent obligation to make good on request any loss or damage suffered by the other party as a result of breach of a contract term, is wide in effect. Where an indemnity clause extends to cover losses suffered by the indemnifying party as well as third parties, it is in effect a kind of exclusion clause. Typically, contracting party where the other party is a subsidiary company within a group, and where the first party is concerned that the subsidiary might not be able to meet its contractual commitments or might be liquidated by the parent if problems were to arise under the contract will demand a parent company guarantee. Alternatively, the first party may have entered into the contract on the basis that the other party is part of a large and reputable group and may wish to avoid the risk of the other party being sold, e.g., to its management.

Ascertainment of Price and Payment terms

The price of the goods may be fixed by the contract, (If the price is to be fixed by an agreement, and no such agreement is in fact come to, the contract will be void: see May and Butcher Ltd. v R (1934) 2 KB 17n HL) or may be determined by the course of dealing between the parties. If the price is not determined, the buyer must pay a reasonable price, and what is a reasonable price is a question of fact dependent on the circumstances of each particular case. Where there is an agreement to sell goods on the terms that the price is to be fixed by the valuation of a third party, and that third party cannot or does not make such valuation, the agreement is avoided, provided that, if the goods, or any part of them have been delivered to and appropriated by the buyer, he must pay a reasonable price for them. Even in the absence of bad faith,a valuer

brought in to fix a term in a contract is liable to be sued damages (See Arenson v Casson Beckman Rutley & Co. (1977) AC 405 (1975) 3 All ER 901, HL, where it was held that an auditor of a private company who on request had valued shares in the knowledge that his valuation would determine the price to be paid for them under a contractor sale was liable to be sued by the buyer or the seller if his valuation was carried out negligently. See also Burgess v **Purchase & Sons (Farms) Ltd (1983) Ch 216 (1983) 2 All ER 4).**

Where such third party is prevented from making the valuation by the fault of the seller or buyer, the party not in fault may maintain an action for damages against the party in fault. Where the contract is for the manufacture of particular goods, or for the supply of goods over a period of time, the price is commonly made subject to variation by reference to increases in the cost, for example, of raw materials and labour. Sometimes contracts will state a price or rate for the undertaking of the contractual obligations, but will fail to state when or how that price is to be paid. Whilst the court may be prepared to interpret such a contract as requiring payment within a reasonable period, it is generally better to state specifically what the payment terms are to be. Retention of Title

The question of retention of title on of has been the subject of much discussion (See e.g. Aluminium Industries Vassen BV v. romalpa Aluminium Ltd (1976) 2 All ER 552, (1976) 1 WLR 676, CA (the Romalpa case) and R. Bradgate Commercial Law (2nd Edn) para 18.4). The limits on the efficacy of such provisions may need to be carefully explained to the seller, proceeding from basic principles. Firstly, what is retention of title and what is its significance? It is the right of the seller to retain ownership of the goods sold until payment, notwithstanding that he has parted with possession of the goods to the buyer. It is vital to bear in mind that, as a general rule, where a contract for the sale of foods has been entered into between the parties for goods in a deliverable state then, under the Sale of goods Act ownership of the goods will pass to the buyer at the time the contract is made, irrespective of whether the goods have been paid for or delivered. It will therefore be obvious that retaining ownership in goods delivered to the buyer but not paid for will be an extremely important right in the event of the buyer becoming bankrupt or going into liquidation. In the event of an insolvency practitioner disposing of the goods or interfering with them, the seller could bring legal proceedings against the practitioner for wrongful interference with the goods and claim damages for their market value. There are, however, a number of practical problems. In

particular, mantelpiece of retention of title clause creates a charge over the goods and (in the case of a corporate buyer) that charge will be void unless registered at the Registrar of Companies. Registration is often considered not practical. So far as the effectiveness of the retention of title), a typical clause will provide further extension on the rights of the seller.

Intellectual Property A significant asset of most businesses is the value of various intellectual property rights, which it owns. These can range from patents to copyright and design rights to protection through registered designs and trademarks to the existence of know-how (both technological and commercial) and other confidential information. If the business is in the high technology market or in a research based industry, these rights are likely to be of substantial value. E.G., if what is being acquired is a pharmaceutical business, patent protection may be vital to the profitability of the business. If the business is a computer software company, the copyright position will be relevant in that it will be important to ensure that the company does in fact have the right to license, use, exploit, etc., the software that it produces. If the business is based substantially on a franchise operation, trademarks and brand names will be fundamental.

Confidentiality

The need for and the scope of, a clause imposing an obligation on one or both parties to keep all matters connected with their agreement confidential will depend on the subject matter and the relationship between the parties. In many cases a short general clause will suffice. Where, however, as part of the agreement sensitive information is supplied by one party to the other (e.g. in a software license, or a company take over or merger), then more detailed provision is called for. The need for secrecy may, for commercial reasons, be so strong that a party, e.g. a vendor of a business, may be advised to insist that the other give a separate detailed confidentiality undertaking before negotiations over the deal are commenced. Usually, the recipient of confidential information is required by the agreement to take certain steps to prevent it becoming public knowledge, for example, to keep in it a secure place when it is not in use, to take all reasonably practicable measures to prevent the information falling into the hands of unauthorized their parties and to limit access to the information to those of his employees who need to know or use it (and who sign a written undertaking to maintain it in confidence). The interests of the recipient are often safeguarded by a proviso that the confidentiality obligation does not extend to such information as it is already a part of the

domain of public knowledge when it is disclosed to him or a s afterwards may become a part of the same through its publication by the discloser of a third party. Parties sometimes forget to include restrictions on use of the confidential information. Such a restriction may be just as important as an obligation of nondisclosure. The duration of the confidentiality obligations, and in particular whether they survive termination of the agreement, should be stated.

Announcements

Companies may often wish to control the issue of public announcements about agreements they have made or are negotiating. Sometimes public statements are required, e.g., if a contracting party is listed on a Stock exchange and is required to notify significant transactions to the Exchange. The wording of the announcement may have an effect on the share price. Contracting parties sometimes agree to the text of a joint press release in the course of the contractual negotiations and attach the final form as a schedule to the contract. Costs and Stamp duty The language stating that each party is to bear its own legal costs is probably most useful in situations where there is a long established practice that one party bear all costs, as e.g., in the case of property leases. In many types of contract such a clause may be thought unnecessary. In transactions in which stamp duty may have to be paid, e.g., conveyances of property and

intellectual property assignments, it may be useful to state which party is responsible for having the relevant documents stamped and for paying the duty. This matter for commercial negotiation, but as it will more often than not be the purchaser who wishes to rely on the stampable document in court; he will more typically be the party, which pays the duty. The court will not admit in evidence documents, which are stampable but have not been duly stamped. Taxation An international sale will attract any applicable exchange controls or customs duties. A sale of goods will constitute a disposal of assets for the purposes of tax on capital gains. It goes without saying that any business transaction must be made to work satisfactorily from a tax point of view, and this will be a major consideration in devising a suitable structure.

Insurance Contracts sometimes include warranties as to the level and scope of insurance cover held by a contracting party and / or obligations on a party to insure against specified risks and / or to arrange for the other party to be added as a named party under the first party's insurance policy. Parties to commercial contracts sometimes misconstrue an obligation on a party to insure against a risk as a statement that party is liable for any losses associated with

that risk. Insurance clauses should not be used as a substitute for statements as to which of the contracting parties bears the risk of a particular event happening. The ability of a party to insure against a risk is a factor to be taken into account by the court when assessing whether an exemption clause is reasonable.

Termination

Sometimes agreements are stated to have a fixed term. In such cases the parties will often intend that the agreement will terminate automatically by expiry at the end of that period and it is better to state this rather than assume that this is implicit from the fixed term. If the agreement may terminate earlier, e.g., under another clause allowing for termination in the event of breach or insolvency, the clause providing for the fixed term should be stated to be subject to earlier termination as provided elsewhere in the agreement. Sometimes agreements allow a party to terminate the agreement on notice to the other party (i.e. without specifying a cause, such as for breach or insolvency). If the agreement is silent as to its term, it may (in some situations) be interpreted as being terminable by either party on giving reasonable notice. To avoid such uncertainties it is desirable to specify the term of the contract.

(1) Termination for insolvency :

It is customary to provide that certain specified kinds of default will entitle the innocent party to terminate the agreement. The description of the particular events, which will constitute such a breach, will vary from contract to contract. The insolvency of a party is almost always stipulated as an event entitling the other party to terminate the agreement. In the absence of such a provision, the bankruptcy or winding up of one party may of itself be insufficient to terminate the contract. It is always advisable to be specific when framing such a provision.

(2) Termination for breach :

The innocent party may be entitled to terminate a contract de futuro (le terminate the contract or bring it to an end as to the future, or rescind it de futuro. Distinguish rescission ab initio for misrepresentation) on any of the following grounds.

(3) An express provision in the contract allows the innocent party to terminate the contract either on the grounds le terminate the contract or bring it to an end as

to he future, or rescind it de future. Distinguish rescission for misrepresentation that the other party has committed a breach listed in the contract as having such an effect or because the happening of some event (including performance by the other party) is a condition precedent to his liability.

(4) In any agreement containing obligations of a continuing nature one party will wish to be able to terminate the agreement if the other party is in serious default. At common law, one party may rescind the contract where the other party has committed a serious or fundamental beach by defective performance or has repudiated the contract. It is always advisable to provide expressly for the circumstances in which either party may treat the contract as at an end. In the absence of such provision it is not always clear whether a particular branch would entitle the innocent party to rescission, each contract will be construed on a case-by-case basis.

Remedies

Rescission for misrepresentation Wherever a party is induced to enter into a contract by a material misrepresentation, whether innocent or fraudulent, he has a prima facie right to rescind abinito, although the contract will normally continue to force unless he so elects. Where a person has entered into contract after a misrepresentation has been made to him, notwithstanding that the misrepresentation has become a term of the contract or the contract has been performed, then, if that person would otherwise be entitled to rescind the contract without alleging fraud, he is entitled to rescind the contract. This right is subject, however, to the power of a court or arbitrator to award damages in lieu of rescission if of the opinion that it would be equitable to do so, having regard to the nature of the misrepresenting and the loss that would be caused if the contract were upheld as well as to the loss to the other party if rescission was permitted.

Repudiation any unequivocal refusal by a contracting party to perform his contractual obligation (including self-induced frustration. As to frustration including self induced frustration) may amount to a repudiation (See further 9 Halsbury's Laws (4th Edn) Para 546 et seq. But repudiation is a serious matter and not to be lightly inferred, see Ross T Smyth & Co Ltd. v T.D. Bailey, Son & Co. (1940) 3 All ER 60 at 71 HL per Lord Wright). The repudiation may be express, or it may be implied, the implication may be made by statute, or in

law, as where a party incapacitates himself from performing his contractual obligations, (As by a supplier wrongfully reselling goods) or completely fails to perform his side of the bargain. (E.g. Gill & Duffus SA v Berger & Co. Inc (1984) 1 All ER 438, Hl, Eg Gill & Duffus SA v Berger & Co. Inc. (1984) AC 382 (1984) AC 382 (1984) if he elects to keep the contract alive, each must perform his own side of the contract, but the innocent party may claim damages by reason of the breach. However, if he elects to rescind, the effect is to discharge both parties from any duty of further performance of the primary promises made under the contract but, whilst the guilty party remains liable for damages for past and future breaches, the innocent party is liable for damages only for past breaches. Damages an action for damages may lie at the suit of the buyer for breach of contract, tort of misrepresentation.

1. Specific enforcement

Two equitable and discretionary remedies may be available. First, in an action for breach of contract to deliver unique, specific or ascertained goods the court may, if it thinks fit, on the plaintiff 's application, by its judgment direct that the contract shall be performed specifically, without giving the defendant the option of retaining the goods on payment of damages. Second, the buyer may obtain an injunction preventing the supplier disposing of those goods to a third party.

2. Damages for breach

This paragraph deals with the situation where a buyer has an action in damages for breach of the sale contract against his seller. The rules here will differ according to whether or not the breach by the seller amounts in law to a failure to deliver the goods.

3. Damages for breach

This paragraph deals with the situation where a buyer has an action in damages for breach of the sale contract against his seller. The rules here will differ according to whether or not the breach by the seller amounts in law to a failure to deliver the goods.

4. Damages for non-deliver

This category covers not only the situation where no goods are delivered at all, but also where the goods tendered by the seller are lawfully rejected and the contract discharged on the grounds that they do not conform to the contract in quantity or quality. The Sale of Goods Act provides that where the seller wrongfully neglects or refuses to deliver the goods to the buyer, the buyer may maintain an action against the seller for damages for non-delivery.

6.4 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 defense 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.

6.5 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,
- 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.[30]

6.6 Civil Liability for Corporate[31]

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

[30] Civil Liberties and the amended Information Technology Act, 2000; The Centre for Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/information-technology-act

[31] Privacy and the Information Technology Act – Do we have the Safeguards for Electronic Privacy? By The Centre for Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- 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.

6.7 Adjudication[32]

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.

6.8 Evidences[33]

[32] Cyber Laws in India (.pdf); retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

[33] Cyber Laws in India (.pdf); retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

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.

6.9 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.

6.10 Summary

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.

6.11 References

1. Introduction to Cyber Crimes in India by VakilNo.1; retrieved from http://www.vakilno1.com/legalviews/cyber-crimes-in-india.html
2. Civil Liberties and the amended Information Technology Act, 2000; The Centre for Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/information-technology-act
3. Criminal Liability Under Changed Law by Praveen Dalal; retrieved from http://www.naavi.org/cl_editorial_04/praveen_dalal/criminal_jan11.htm
4. Chapter-9 Legal Issues by Reserve Bank of India; retrieved from http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=624
5. Privacy and the Information Technology Act – Do we have the Safeguards for Electronic Privacy? By The Centre for Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy
6. Cyber Laws in India (.pdf); retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

6.12 Check your progress

1. Adjudication powers and procedures have been elaborately laid down in _____.
2. _____ of IT Act deals with the aspect of compensation for failure to protect data.
3. In India we have both _____ and _____ laws.

4. _____ with dishonestly receiving stolen computers or other communication device.

6.13 Answers to check your progress

1. Section 46
2. Section 43A
3. Substantive, procedural.
4. Section 66B

6.14 Terminal Questions

1. Discuss the concept of accrued liability and procedural law.
2. Explain ‘data protection’ in detail.
3. What do you mean by privacy and surveillance?
4. What are the civil liabilities for corporate? Discuss.
5. Describe the term ‘pre-censorship’.

Unit-7

Internet Ownership and Standards

Objectives:

This unit has been prepared to acquaint you with

- Ownership of Internet;
- What standard governs the internet?

Structure

7.1 Introduction

One of the advantages of the Internet over other methods of communication and commerce is that it enables access to a much wider, even a worldwide, audience. Spatial distance and national borders are irrelevant to the creation of an Internet business, many of which are conceived for the express purpose of expanding sales horizons across borders. In a sense, a person can be everywhere in the world, all at once. This ease of communication raises a vital legal question, however: when a person puts up a website on his home server and allows access to it from all points on the globe, does he subject himself to the governance of every law- and rule-maker in the world? Under the current system, in order to decide what state's or nation's laws govern disputes that arise over Internet issues, a court first must decide "where" Internet conduct takes place, and what it means for Internet activity to have an "effect" within a state or nation. Even apart from the Internet, this border-

centric view of the law creates certain difficulties in an economy moving toward globalization. Entire bodies of law have been developed by every nation to deal with the resolution of international conflicts of law, conflicts that arise when geography and citizenship would allow a dispute to be decided by the laws of more than one country, and the laws of those countries are not consistent with each other. Conflicts of law are particularly likely to arise in cyberspace, where the location of an occurrence is never certain, where ideological differences are likely to create conflicting laws, and where rules are made not only by nations and their representatives, but also by sub-national and transnational institutions.

7.2 The test currently in force

A. In the United States

A court does not have power over every person in the world. Before a court may decide a case, the court must determine whether it has "personal jurisdiction" over the parties. A plaintiff may not sue a defendant in a jurisdiction foreign to the defendant, unless that defendant has established some relationship with that forum that would lead him to reasonably anticipate being sued there.

In the U.S., the Due Process clause of the Constitution's Fourteenth Amendment sets the outermost limits of personal jurisdiction. If a party has substantial systematic and continuous contacts with the forum, a court may exercise jurisdiction over a party for any dispute, even one arising out of conduct unrelated to the forum. This is known as general jurisdiction. For example, a corporation or person can always be sued in its state of residence or citizenship or its principal place of business, regardless of whether or not the claim arose there. If a party is not present in the state or does not have systematic and continuous contacts with the state, courts may exercise jurisdiction over a party for causes of action arising out of his contacts with the state, or arising out of activities taking place outside the state expressly intended to cause an effect within the state. This "effects" test is described from the American Law Institute's Restatement (Second) of Conflict of Laws 37 (1971), which provides:

"A state has power to exercise judicial jurisdiction over an individual who causes effects in the state by an act done elsewhere with respect to any cause of action arising from these effects unless the nature of the effects and of the individual's relationship to the state make the exercise of such jurisdiction

unreasonable."

To do this, the court must look to the state's "long-arm" statute, which sets the parameters for the state's exercise of its constitutional power to govern conduct by non-citizens (including both Americans and foreigners). Long-arm statutes vary widely from state to state. For example, Arizona grants the broadest possible freedom to its courts: "Arizona will exert personal jurisdiction over a nonresident litigant to the maximum extent allowed by the federal constitution." New York, on the other hand, gives a more restricted and specific charge to its courts with its statute, which allows personal jurisdiction over those who transact business or commit a tortuous act within the state of New York, and over those who commit an act outside the state that could reasonably be expected to have a tortuous effect within New York. The Federal courts have the equivalent of a long-arm statute of their own, in Federal Rule of Civil Procedure 4(k) (Rule 4(k)), which provides three basic grants of jurisdiction. First, it authorizes federal courts to "borrow" the long-arm statute of the state in which the federal court is located. Second, Rule 4(k) authorizes federal courts to exercise grants of personal jurisdiction contained in federal statutes, such as the federal securities and antitrust law, which have their own jurisdiction provisions. And third, Rule 4(k)(2) grants long-arm jurisdiction in an international context, within the boundaries of the Constitution, over parties to cases arising under federal law who are not subject to the jurisdiction of any particular state. The concept of being able to have minimum contacts with the United States as a whole has profound implications for the Internet and international jurisdiction. Users all over the world, without establishing contacts in a particular state, could establish contacts with the entire country with nearly every foray into cyberspace.

In order to be subject to personal jurisdiction in a state that is not his domicile, not only must a person fit under the ambit of the state's "long-arm" statute, but also the state's jurisdiction must be valid under the Due Process Clause of the Fourteenth Amendment. The Supreme Court set the standard for constitutional exercise of jurisdiction in International Shoe Co. v. Washington. Pursuant to the Due Process Clause, a nonresident defendant may not be sued in a forum unless it has first established sufficient "minimum contacts with [the forum] such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." In addition, the nonresident's "conduct and connection with the forum [must be] such that he should reasonably anticipate being haled into court there." This test relies on

courts to decide, according to "traditional notions of fair play and substantial justice," what contacts are sufficient.

Courts will generally hold that contacts are sufficient to satisfy due process only if the nonresident "purposefully availed" itself of the benefits of being present in, or doing business in, the forum. According to a the plurality of the Supreme Court in Asahi Metal Industry v. Superior Court, a connection sufficient for minimum contacts may arise through an action of the defendant purposefully directed toward the forum State. The placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the Forum State, but advertising or marketing in the forum state may fulfill the deliberate availment requirement. There must be clear evidence that the defendant sought to serve the particular market.

If the minimum contacts test is met, a court may only exercise jurisdiction if it is "reasonable" to do so. In determining reasonableness, a court must weigh and consider the burden on the defendant to litigate in the forum, the forum state's interests in the matter, the interest of the plaintiff in obtaining relief, efficiency in resolving the conflict in the forum, and the interests of several states in furthering certain fundamental social policies.

In sum, under U.S. law if it is reasonable to do so, a court in one state will exercise jurisdiction over a party in another state or country whose conduct has substantial effects in the state and whose conduct constitutes sufficient contacts with the state to satisfy due process. Because this jurisdictional test is ambiguous, courts in every state of the U.S. may be able to exercise jurisdiction over parties anywhere in the world, based solely on Internet contacts with the state.

B. Internationally

There is little dispute that nation-states can prosecute Internet users (or anyone else, for that matter), whatever their location, for revealing national secrets, falsifying official documents, or inciting war. These activities threaten national security, wherever they are committed, and therefore fall under international standards for jurisdiction. Similarly, it is a universal crime to publicly incite torture or genocide. These universal offenses may be prosecuted extraterritorially by any nation, regardless of the citizenship or location of the user.

These are easy cases, however. Nations may also be interested in enforcing non-universal laws extraterritorially; for example, In Germany, it is

illegal to import distribute material espousing a Nazi or Neo-Nazi viewpoint. Such material is not difficult to find in USENet or on the World Wide Web. German authorities may be interested not only in interpreting German laws to classify Internet viewing as "importation" of material, but also (in part because of the difficulty of locating those who break an importation statute without leaving their own homes) in prosecuting those who make such material available to Germans via the Internet. If German authorities attempted to prosecute a U.S. citizen r resident for such an offense, however, they would be met with great opposition by the U.S., which certainly would not enforce any judgment against the U.S. citizen in such a case, because the German statute violates U.S. Constitutional principles. Under U.S. law, because it would be prohibitively difficult to prevent German users from viewing such a site and therefore the result of such a prosecution would be to chill otherwise legal (if unpleasant) speech in the U.S. Under the current system, it is possible to envision that German courts may have jurisdiction over Americans who publish such material, even though the material may not be "purposefully directed" (one interpretation of the American standard) toward Germany in the way a mailing of flyers would be.

As discussed above, U.S. courts apply the same "effects" test to foreign parties as to American parties. If minimum contacts exist, parties from other countries may be haled into court in the United States just as parties from one state may be haled into another. Similarly, Americans may be tried by courts in other countries depending on the rules of that country. Although each country's laws are different, most rely on some sort of "effects" test resembling the U.S. test, whereby a party is subject to jurisdiction in a place where his conduct has an effect. This jurisdiction traditionally is subject to a "reasonableness" test. According to section 421 of the Restatement (Third) of the Foreign Relations Law of the U.S., exercise of jurisdiction is generally reasonable if the party is a citizen, resident, or domiciliary of the state, or if:

(g) the person, whether natural or personal, has consented to the exercise of jurisdiction;

(h) the person, whether natural or juridical, regularly carries on business in the state

(i) the person, whether natural or juridical, had carried on activity in the state, but only in respect of such activity;

(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or

(k) the thing that is the subject of adjudication is owned, possessed, or used in the state, but only in respect of a claim reasonably connected with that thing.

This standard differs somewhat from the U.S. standard for interstate exercise of jurisdiction; for example, transitory presence (known as "tag" jurisdiction), accepted in the U.S., is not generally accepted as a method of international jurisdiction.

Every nation has an obligation to exercise moderation and restraint in invoking jurisdiction over cases that have a foreign element, and they should avoid undue encroachment on the jurisdiction of other States. Although countries are given great discretion in deciding whether to exercise jurisdiction over conduct in other countries, international law dictates that a country exercising its jurisdiction in an overly self-centered way not only contravenes international law, but can also "disturb the international order and produce political, legal, and economic reprisals."

Based on this traditional moderation, and the relatively high threshold of the "reasonableness" standard discussed above, it is unlikely that foreign nations will have the sort of long-arm power over citizens of other nations as states have over citizens of other states within the U.S. today. Scholars have suggested that individual persons and small commercial entities whose only contacts with a nation are on-line are, in all likelihood, more insulated from international jurisdiction than they are from interstate jurisdiction. This is largely speculative, however, because international Internet jurisdiction cases have thus far been rare, and nations have not hesitated to pass laws conferring global jurisdiction for Internet activities.

7.3 Application of the "Effects" Test to the Internet

A. In the United States

The Supreme Court has not discussed the impact that technology might have on the analysis of personal jurisdiction. Lower courts, on the other hand, have explored the question of cyberspace jurisdiction. While most have held that merely creating and hosting a website available to all does not subject a person to general jurisdiction everywhere in the U.S., they diverge widely as to whether the presence of such a site will lead to specific jurisdiction over the

party for the purposes of disputes arising from the website. Some decisions suggest that a court may obtain personal jurisdiction over a non-resident defendant whose sole contact with the forum state arose through the Internet. Examples of these include: CompuServe, Inc. v. Patterson, Zippo Manufacturing v. Zippo Dot Com, Inc., Panavision International, L.P. v. Toeppen, and Maritz, Inc. v. Cybergold. In each of these cases, Internet contacts with the forum state exceeded those of a passive website: In CompuServe, the defendant knowingly reached out to and did business with CompuServe, knowing that CompuServe was an Ohio corporation. In addition, the dispute arose out of contacts with the forum state. In Zippo, the defendant's site required participants to submit address information in order to receive a news service; therefore, the site operators knowingly transacted business with residents of the forum state, where the plaintiff was headquartered. In Panavision, the defendant had set up his web site as part of a "scam" to make the plaintiff purchase the domain name from him, and as such had intentionally directed his actions toward the plaintiff's home state. In Maritz, the defendant's site invited users to send and receive information about services it offered, and the defendant company had send information to over 100 users in the forum state. The court found that "[a]lthough [defendant] characterizes its activity as merely maintaining a 'passive website,' its intent is to reach all Internet users, regardless of geographic location."

Two other recent decisions, in declining to exercise jurisdiction, support the notion that passive Internet sites are not sufficient to support jurisdiction. In McDonough v. Fallon McElligott, Inc., a Minnesota defendant had displayed plaintiff's photographs on the Web without plaintiff's consent, in possible violation of California copyright and unfair competition laws. The Southern District of California held that: "Because the Web enables easy world-wide access, allowing computer interaction via the Web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists . . . . Thus, [having] a Web site used by Californians cannot establish jurisdiction by itself." Similarly, in Benusan Restaurant Corp. v. King, the Southern District of New York held that the operator of a small Missouri jazz club called "The Blue Note" did not subject it to New York's trademark laws by erecting an advertising site on the Web. The New York district court's holding in Benusan is at direct loggerheads with the District of Connecticut's holding in Inset Systems, Inc. v. Instruction Set, Inc. In Inset, a party utilizing the trademark of another

company for its domain name and "800" number was subject to jurisdiction in the home of the party whose mark was infringed. Also in seeming conflict with Benusan and most other U.S. interstate Internet jurisdiction cases, the Federal Circuit found in Graphic Controls Corp. v. Utah Medical Prods., Inc., that a Utah corporation's activities, which included having an open-access website for ordering goods, having an "800" number, having meetings in New York unrelated to the cause of action, and sending "cease and desist" letters to party in New York, did not constitute minimum contacts with New York. In similar conflict with the above cases, the Southern District of New York held that creating a commercial and interactive (though not yet operational at the time of litigation) website that was available to, and used by, New York residents was not in itself enough contact to subject a publisher to New York jurisdiction in Hearst Corp. v. Goldberger. The District court found that exercising jurisdiction would violate traditional notions of fair play, and noted that the site operator did not purposefully direct his activities toward New York.

The disagreements between the cases above illustrate some of the variety among courts as to the proper approach to take when dealing with Internet jurisdiction. Approaches differed greatly, even among some of the above cases having similar final outcomes. States have not regularized an approach to the Internet, preferring to analogize it to real space. Erecting a website has been compared to publishing in a widely distributed general-interest magazine or putting an item (with the capacity to travel) in the stream of commerce by selling it locally. As the above illustrate, courts seem to be taking an approach resembling that recently laid down by the Ninth Circuit Court of Appeals in Cybersell, Inc. v. Cybersell, Inc., which held that the mere presence of a passive website on the Internet does not constitute the minimum contacts needed to subject a person to the jurisdiction of every court and that "something more," either interactivity or purposeful direction, is needed to justify jurisdiction. What degree of interactivity is required to constitute minimum contacts, however, remains largely unclear from case law. Under the rule set forth in Cybersell, a court would decide whether a website creates minimum contacts by examining the degree to which the site is commercial and interactive, and the degree to which the site is directed at citizens of the forum state. The more interactive a site is (i.e. the more exchange of information is possible between the site and the user), and the more commercial the site's nature, the more likely a court is to find that contact exists between

the site owner and the distant user. Similarly, the more the site is directed at an audience in the forum site or designed to harm citizens of the forum state, the more likely a court will be to find that purposeful availment has occurred. Still, the Supreme Court has not addressed the issue of persona jurisdiction in cyberspace and many details still remain unresolved.

B. Internationally

U.S. courts have, basically, shoehorned Internet cases into the same jurisdictional rules that they use for non-Internet cases, with the result that U.S. courts lean toward limiting jurisdiction, regulating only sites that intentionally direct themselves into the U.S. in some way. Other countries have not limited their courts so. Several examples illustrate that jurisdictional issues are at least as severe and jumbled in the international context as they are within the domestic U.S. In the United Kingdom, the Financial Services Act of 1996 makes it a criminal offense to place investment ads in the U.K. unless they are issued or approved by the Financial Services Authority (FSA). In early 1998, the FSA notified the national U.S. mutual fund association that mutual fund Web sites which can be brought up on a screen in the U.K. are considered to have been issued in the U.K. This could have had a profound impact on the way in which U.S. mutual fund sites operated, however, the FSA stated that it would not take enforcement action against U.S. companies that complied with certain FSA regulations, including placing disclaimers or warnings on their Web sites.

Germany has passed a sweeping law that subjects any Web site accessible in Germany to German law, holding Internet service providers (ISPs) liable for violations of German content laws if the providers were aware of the content and were reasonably able to remove the content. This followed the settlement of a well-publicized incident between Germany and CompuServe, in which German authorities threatened to prosecute CompuServe for allegedly pornographic news groups. In response to the German threat, CompuServe blocked access to those newsgroups to all users, approximately 4 million worldwide. Later, CompuServe restored access and distributed free software for blocking pornography. This caused CompuServe's indictment for aiding in the distribution of pornography and computer games. Prosecutors charged that CompuServe did not do enough to block Germans from accessing the material.

Malaysia's new cyberspace law also extends well beyond the borders of Malaysia. The bill applies to offenses committed by a person in any place, inside or outside of Malaysia, if at the relevant time the computer, program, or data was either (i) in Malaysia or (ii) capable of being connected to or sent to or used by or with a computer in Malaysia. The offender is liable regardless of his nationality or citizenship.

7.4 Conflicts of Law

As mentioned above, the Constitution and states' long-arm statutes may permit court jurisdiction over out-of-state conduct, depending on the specific long-arm statute and the conduct involved. This means that many states may have concurrent jurisdiction over the same conduct. A similar situation exists in the international context. Because it is generally accepted as a matter of international law that nations may govern conduct of citizens of the nation taking place outside the nation, conduct by non-nationals that take place elsewhere but has significant and intended effects in the state or nation, conduct that threatens the sovereignty or security of the nation, and conduct that constitutes a universal crime such as torture and genocide, many situations may arise in which several nations' laws could govern the same conduct. To use a real-space example, imagine that A (an American shipping company) ships a batch of B's widgets from New York to B in Belgium, by way of France. The widgets are damaged during the French stopover and that this damage gave rise to a cause of action in tort between A and B. Assuming that A had significant enough contacts with both France and Belgium to warrant jurisdiction in both courts, B could sue A in the U.S., in France, or in Belgium, depending on which legal system would treat B more favorably. Additionally, B could sue in U.S. court but request that the court apply Belgian law to the dispute, or sue in Belgian court but request that the court apply French law, or any other combination of courts and laws.

The many applicable laws will not necessarily be substantively compatible. Different states and nations will have different interests and each will want its laws to govern each dispute. This situation becomes extremely poignant when laws are not only inconsistent, but also incompatible; for example, in some states of the U.S., it is illegal to provide or engage in Internet gambling, but in Liechtenstein, such gambling is government-sponsored. Although the situation of inconsistent laws occurs with moderate frequency now (especially in the antitrust and securities fields) it is likely to become even

more common as cyber-commerce becomes more prevalent. This is because, in cyberspace, cross-border transactions are no more difficult than transactions with local parties.

When conflicts of law arise, courts must decide which law will govern. A court need not decide a dispute according to its own law; for example, a court deciding a dispute arising out of an automobile accident in another state would be likely to apply the driving standards of the state where the dispute arose, rather than of the forum state. Several methods exist to aid courts in the decision between laws. Historically, U.S. courts decided a dispute according to the law in the lex loci delicti, the "place of the wrong." In transnational cyberspace, however, the place of the wrong might be any of the nations that are on-line. There is no lex loci delicti.

The Restatement (Second) of Conflicts of Law rejected this historical formulation, preferring the so-called "most significant relationship" test, which values:

(1) the needs of the international system;

(2) relevant policies of the nation in which the suit was brought;

(3) the relevant policies of all interested states;

(4) justified expectations of the parties;

(5) certainty, predictability, and uniformity;

(6) and ease of administration.

Several other approaches to choice of law have also been posited and accepted by some courts. The "center of gravity" approach, first adopted by the Court of Appeals of New York, might be characterized as a simplified version of the "most significant relationship" test of the Second Restatement. This approach authorizes courts to look at all the existing contacts between the various parties to a suit and various jurisdictions. Ultimately, the court should choose the law of whatever jurisdiction is most closely tied to the case.

Legal scholar Brainerd Currie espoused the "interest" approach, which encouraged courts to look to the history of the applicable laws and, if the laws of one state could be applied without impairing the other state's interests, those laws were to apply. In the case of a true conflict, in which one state's interests would always be impaired, Currie suggested using the law of the forum. California has accepted this approach, but instead of automatically applying the law of the forum in true conflicts cases, applies a "comparative impairment" analysis and applies the law of the state that creates the least impairment.

Finally, Professor Robert Leflar has devised a test in which courts consider :

1) predictability of result
2) maintenance of interstate and international order
3) simplification of the judicial task
4) advancement of the forums governmental interests, and
5) application of the better rule of law.

Currently, U.S. states and the U.S. itself take a variety of approaches; none of the above approaches have been universally accepted.

Interestingly, most approaches other than the "place of wrong" approach eliminate the need to decide "where" the conduct in question occurred before deciding what law governs (although determining the location of an action may help create the list of nations' laws from which to choose). As the few reported cases show, however, courts may ignore traditional choice-of-law principles entirely and simply apply forum law to Internet-related disputes. Indeed, at least one state, responding to the problem of Internet-based gambling, has announced an intention to apply its own law to lawsuits resulting from in-state Internet contacts. The Minnesota Attorney General's office, has interpreted existing Minnesota law to prohibit all forms of on-line gambling, and noting that "[g]ambling is just one example of illegal activity on the Internet" and "the same jurisdictional principles apply with equal force to any illegal activity." Courts have tended to apply the law of the forum state in Internet cases, without discussion.

It should be noted that many Internet activities are commercial and that many of these involve contractual transactions. These contracts may contain choice-of-law clauses defining what state's law will govern any dispute arising out of the transaction. Most ISPs, for example, include choice of law clauses in their service agreements; such clauses may greatly simplify choice of law questions on the Internet, as choice of law clauses are, for the most part, honored as a matter of international law. Many Internet activities are not commercial or even transaction-oriented, however, and choice of law clauses may not cure problems arising from non-transaction-oriented activities. Case law does not indicate what route courts might take in resolving true choice of law disputes arising from such activities. One commentator has suggested the creation of a choice-of-law treaty for the Internet.

7.5 Practical Implications of these laws: Looking to the future

Many questions remain about how courts will fit the Internet into the current system of jurisdiction. For this reason, people do not know what laws to live by. Although most people know the laws of their domicile state, many do not know the laws of states with which they will be interacting; therefore, under the current system, it remains entirely possible that a person could be haled into court in a foreign land for something that is perfectly legal in his domicile. Simply put, the "effects" test doesn't work. It is true that states and nations are perfectly within their power in prosecuting foreign parties who provide illegal services (for example, a Nevada site that provides gambling to a Minnesota resident), and foreigners who commit crimes (for example, an American who posts names of businesspeople on a site available to Chinese dissidents). However, the architecture of the Internet makes it easy for people to obfuscate their identity and location and it is therefore impractical, under the current architectural regime, to make sites provide and deny service based on a person's identity; yet, that is exactly what the current legal system requires. Most importantly, under the current regime, people can unwittingly open themselves to liability, by posting information on the Web that they consider proper. For example, a local company with the same name as a different company across the country and thereby expose itself to trademark liability; or an American could put up a site containing photos of women in short skirts, thereby exposing himself to criminal liability in countries under Islamic law.

If the current legal system is to maintain effective and fair control over the Internet, courts all over the world will have to make a clear move toward a new test for jurisdiction, and a consistent test for resolving choice of law disputes. If courts could agree to exercise jurisdiction based on an effects test with a much stronger element of purposeful availment than exists in the current system, the current style of legal governance might be able to serve the Internet in an effective and consistent way, without the excessive and unpredictable elements that it currently suffers from. For the purposes of fairness, mere awareness that a site could be accessed at a location would not be enough to trigger jurisdiction; rather, in order to be subjected to jurisdiction in a place other than his domicile or its primary place of business, a party would have to display intent to reach the audience in that location through advertising or special targeting subject matter, or a positive awareness of an audience's locations by way of interactions involving the exchange of information about real space location. Under such a system, a party would still be subject to

jurisdiction in its home state or nation, but not in a foreign jurisdiction unless the party sought out an audience in that foreign jurisdiction. Such a system would put the burden on state and local authorities to prevent the viewing of illegal material and to focus on laws regarding the use of illegal material, rather than laws the provision of such material. As they are today, transactions would be susceptible to the jurisdiction of the domiciles of all parties involved and any jurisdiction in which the transaction was definitively intended to have an effect.

Use of Internet and Computers by Terrorists[34]

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

The Scenario

The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people. For e.g. one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible. Terrorists also use physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. They also use virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, G space etc.

The law

Terrorists are covered by conventional laws such as Indian Penal Code and special legislation relating to terrorism.

Who is liable?

Terrorists as well as those who help them to protect their information are liable. If email service providers do not assist the law enforcement personnel in the investigation then they are also legally liable.

The motive

[34] Real world cybercrime cases by Rohas Nagpal, Asian School of Cyber Laws; retrieved from http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/real-world-cyber-crime-cases.pdf

Keeping terrorism related information confidential. Secure communication amongst terrorist group members.

Modus Operandi

The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

7.6 Misuse of technology

Cases involving misuse of Internet / Emails is not maintained separately by Government. However, as per the general cybercrime data maintained by National Crime Records Bureau, a total of 217, 288, 420 and 966 Cyber Crime cases were registered under Information Technology Act during 2007, 2008, 2009, 2010 respectively, thereby showing an increasing trend. A total of 339, 176, 276 and 356 cybercrime cases were reported under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009, 2010 respectively.

7.7 Summary

In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well. The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents.

7.8 References

1. Cyber Laws in India retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf
2. India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective by Rohit K. Gupta; retrieved from http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective
3. Seth Associates (Advocates & Legal consultants); retrieved from http://www.sethassociates.com/criminal-liability-for-misuse-of-information-technology.html
4. Alert India.com, retrieved from http://www.alertindian.com/node/5

5. Cyber Crimes: Law and Practices (.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
6. Seminar and Workshop on detection of cybercrime and investigation by Justice K.N. Basha; retrieved from http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf
7. Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6
8. Real world cybercrime cases by Rohas Nagpal, Asian School of Cyber Laws; retrieved from http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/real-world-cyber-crime-cases.pdf

7.9 Check your progress

1. Section 420 of IPC deals with _____and dishonestly inducing delivery of property
2. _____ is a term used to describe the legal issues related to use of communications technology.
3. _____ deals with power to adjudication under IT Act, 2000.
4. Section 464 of _____ refers in matter of making a false document.
5. Section 499 of Indian Penal Code deals with _____.

7.10 Answer to check your progress

1. Cheating
2. Cyber law
3. Section-46
4. Indian Penal Code
5. Defamation

7.11 Terminal Questions

1. Describe defamation as per discussed in Indian Penal Code.
2. Discuss in detail section 420 of Indian Penal Code.
3. Explain how terrorists use internet technology to commit crime?
4. Discuss power of adjudication.
5. Explain Sony sambandh case under Indian Penal Code?

Unit-8
Cyber Space, Democracy and National Sovereignty

Objectives:

This unit has been prepared to acquaint you with

- Sovereignty and the Role of Government in Cyberspace;
- Purpose and Deletion and Blocking of Contents on internet.

Structure

8.1 Introduction :

One of the central elements of thinking about internet policy was that the role of government in this new domain should be minimal, both because this was the best thing to do and because many obstacles prevent national governments from extending sovereign control into cyberspace. This belief had profound and ultimately damaging implications for security. A reexamination of these beliefs suggests that they are best seen as a product of their time rather than immutable characteristics of cyberspace. Ideology, culture, and business practices help explain the initial understanding of cyberspace and government's role in it.

Many of the assertions produced to support a limited role for

government do not hold up to scrutiny. The belief that the internet had initiated a period of rapid, fundamental economic change was taken as implying that "the digital economy moves too quickly and requires too much flexibility for the processes of government to be, in most cases, successful in relating to it."[1] This conflates evolving business models with fundamental change. The argument that technology evolves too rapidly to be regulated is true only if we lack perspective. The flood of new applications and devices can appear bewildering and overwhelming, but the speed of technological change has been overstated. There have been four technological epochs in the last forty years: the mainframe era, the advent of the PC, the internet, and now a move into mobile and what is often called "cloud computing." This is a rapid rate of change when compared.

James A. Lewis is a Senior Fellow and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS). His research focuses on cyber security, intelligence reform, space programs, and economic change. He previously served as a member of the U.S. Foreign Service and Senior Executive Service and is the author of multiple publications, including *Securing Cyberspace in the 44t h Presidency* (2008)

8.2 Objective

The internet began as a U.S. government enterprise, created for defense and research purposes. The steps taken by the Federal Government in the early 1990s in opening this government-controlled network of networks to private activity profoundly affected internet governance. The U.S. government opened the internet to the public in a period of substantial political change, shaped by the triumph of market economies during the cold war and reinforced by the trend in many industrialized nations towards deregulation, particularly in telecommunications.[2] The policy decisions made in this larger political context were reinforced by the general anti-authoritarian, non-hierarchical and anti-government beliefs held by many internet pioneers. The result was a conscious decision in the United States to minimize government role, as "private-sector action is preferable to government control."[3] The growth of the internet also coincided with (and was intimately involved in) the growth of a global economy. National borders became less relevant (and national policies less effective) in this new economic environment. The erosion of sovereignty and the possible demise of the Westphalia state system brought on by globalization strongly affected views on internet governance held by policy makers,

technophiles, and the internet community.

The decision by the U.S. government to turn over most governance functions to the private sector were also shaped by the assumptions of the dot-com era, when internet pioneers proclaimed repetitively that the internet and the World Wide Web were new phenomena; old rules did not apply because it is untrammeled, borderless, and without need for traditional government.[4] Such pronouncements affected policy makers in many countries, who feared that government intrusion would damage adoption of the new technology and condemn them to a secondary economic status. The debate in the United States and in its European allies over the control of encryption products reinforced the emphasis on private sector leadership. Other industrial nations mirrored U.S. efforts to impose a single encryption technology and to create a national regulatory scheme for the use of encryption, which led to technological dead ends and won little public support. The effort to mandate use of the clipper chip was (and remains) a powerful argument for minimizing the government's role in prescribing technological solutions. The conceptual gap between internet security and commercialization in U.S. policy-making was so large that the Clinton White House set up two separate working groups: one on security led by John Deutsche, the Director of Central Intelligence and one on commercialization led by Ira Magaziner, Clinton's advisor on health care. Coordination between the two groups was often patchy and at times was marked by a degree of hostility and competition.[6]Assertions about sovereignty and the role of government in cyberspace have taken on new importance in recent years. Some reflect a growing awareness of threats and vulnerabilities, but most of it stems from the realization that the internet has become a vital component of economic activity and national security. This dependence has brought growth and greater efficiency in business, research and government.[7] The United States has woven computer networks into so many of its economic activities The internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. Like other past innovations—airplanes, cars, and steam engines—the appeal and the benefits are so great that we have rushed to adopt the internet despite serious safety problems.[8] The global connectivity of the new infrastructure amplifies these problems, as the speed of internet connections means that geographical distance provides little in the way of protection. For earlier technologies, safety came about through innovation driven by government mandates, and by agreements among states. The same process of

maturation is necessary to secure cyberspace, but this will require shedding some of our old ideas about its nature. There is a reluctance to acknowledge the ideological blinders that shape our views on the nature of the internet, the role of government, and the limits of sovereignty. The early architects and thinkers of cyberspace in the first flush of commercialization downplayed the role of government.[9] Their vision was that cyberspace would be a global commons led and shaped by private action, where a self-organizing community could invent and create. This ideology of a self-organizing global commons has shaped internet architecture and policy, but we must now recognize its inadequacy.[10]

Second, in the absence of government intervention, adequate security will not be provided.[11] Cyber security is a public good, goods are those that benefit all of society but whose returns are difficult for any individual to capture. The private sector does not adequately fund public goods because returns to the individual investor may be inadequate, even though the returns to society are great; we can add cyber security to this list of public goods. The combination of unplanned global access, porous technologies, and weak governance makes this newly critical infrastructure exceptionally vulnerable. As the United States' reliance on the internet increases, so does its vulnerability to remote exploitations and attacks. That the technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but at the price that anyone with malicious intent can easily exploit these networks. Beliefs shape actions and understanding. For the internet, these beliefs were a mixture of libertarianism, anti-authoritarianism, and belief in a New Economy, strongly supported by business interests who sought to limit regulation and liability. [12] The resulting "architecture" for cyberspace reflects these beliefs and is now under challenge. Perhaps more importantly, they limit our ability to define both problems and solutions. An approach to governance constructed on this foundation was not inevitable, but a matter of choice. Those choices, made largely by U.S. citizens, can be undone, especially as other nations gain influence in shaping cyberspace.

An uptake of new network technologies made great advances in numbers and in geo-graphic spread in the 1990s. The culture that shaped this uptake was largely American; a blend of science and engineering cultures with a strong dose of West Coast libertarianism contributed to this culture. While this image and mindset is appealing, it is also fading. The modern internet architecture, standards, and protocols originate from the United States and date

back to the 1990s. As manufacturing spreads to other countries with political objectives that are less dominated by free market doctrine, the ability of U.S. citizens to "build in" their beliefs into the technology is diminished. Other states often also are less retrained about government intervention and industrial policy, as they see the risk of an unregulated infrastructure as unacceptable .The designers and theorists of the internet built the network to reflect their values: the internet was open and non-hierarchical, as well as somewhat antiauthoritarian and anti-government. Theorists such as Kevin Kelly, Howard Rheingold, and John Perry As Steven Levy described, "the engineers and programmers who loved computers and had become politicized during the anti-war movement were thinking of combining the two activities."[15] Their ideas were influential and, to a degree, shared by officials in the Clinton administration responsible for commercializing the internet. Given the central role of the United States in the 1990s in shaping cyberspace, these ideas helped determine the future path of internet governance.[16] The outcome was a conscious decision by the United States to minimize government's role, as "private-sector action is preferable to government control."[17]

Certainly, in some instances, such as the Internet Engineering Task Force (IETF) or the Open Source Software Movement, this vision of an open, nonhierarchical com-munity has worked exceptionally well. This open, non-governmental approach likely accelerated creativity and the adoption of the technology, but the amorphous and, at times, anonymous global collective of millions of individuals has overwhelmed the capacity for self-governance.

The anti-authoritarian aspects of internet culture were strengthened by the concept of a New Economy, which seemed to reinforce the point that old structures were inappropriate for cyberspace. In the New Economy, old economic rules seemed to no longer apply as economic activity in the 1990s transitioned, supposedly, to an economy based on the exchange of ideas and information. A commonly held view in Silicon Valley was that Washington was largely irrelevant to this new world.

The strength and influence of these ideas in shaping internet governance rests on linkages among the beliefs and perceptions held by internet pioneers. These link-ages have not yet been fully explored. The beliefs held by the individuals who made internet policy were based on their political experiences in previous decades. In this case, the original governance bodies of the internet, such as the IETF, were formed along the lines of self-organizing communities or non-governmental entities, such as the Internet Corporation for Assigned

Names and Numbers (ICANN) in accordance with the "New Economy" mindset.

Additionally, some of the crucial figures establishing the governance framework for cyberspace were themselves college radicals or were closely linked to politics of the 1960s.[18] One of the most important of these was Ira Magaziner. Magaziner directed the Clinton administration's planning to commercialize the internet, and was himself once a college activist. Magaziner's views are complex and nuanced, but his preference was for a "market driven approach . . . [that] was a bottoms up kind of medium that should not be over-regulated."[19] As he put it, "I think a model of industry self-regulation and of industry codes of conduct and decentralized governance fits better for the Internet age...That is part of the new model that we think will govern in the digital age."[20]

"The Federal Government should recognize the unique qualities of the Internet including its decentralized nature and its tradition of bottom-up governance. Existing laws and regulations that may hinder electronic commerce should be revised or eliminated consistent with the unique nature of the Internet." White House Memorandum on Electronic Commerce, July 1997

The commercialization of the Internet came to a head during the high tide of regulation. The experience of central governments in using Keynesian tools to manage their economies led to the recognition that control ran counter to economic growth. Regulated industries were often inefficient in their use of resources and in their delivery of goods and services. The long cycle of deregulation in the telecommunications industry was particularly important in shaping the views of internet pioneers. Deregulated telecom companies performed better than government owned firms, and it is not surprising.

8.3 Sovereignty and the Role of Government in Cyberspace

Telecom deregulation, however, was an inadequate model for the Internet, as it was concerned with ownership and the introduction of market forces into the supply of telecom services within a larger regulatory context that sought to ensure security and quality of service.

Voluntary self-regulation has strong roots in U.S. political culture. As the United States evolved into an urban, industrial society, reformers found the concept of highly trained professionals exercising stewardship over public policy and transforming public policy issues into scientific, technical and managerial problems more attractive than the dubious electoral politics of the

1900s. The approach emphasizes "engineering efficiency" over "inefficient" democracy and a dependence on private sector initiatives to meet public needs, on the grounds that small groups of experts, accountable to scientific principles rather than the broad public, are more likely to arrive at effective solutions. The center of this philosophy was Herbert Hoover's Commerce Department, and there is some irony that 70 years later, it was the department he founded to encourage efficiency and private-led expertise that promoted the self-governance policies that shaped the commercial internet in its inception.

Three general principles for internet policy emerged from this culture. First, policy should be technology-neutral. Second, development of policy was to be industry-led, as part of a public private partnership where government's role would be to provide a in a failure to distinguish between those activities where self-regulation is best and those where it is inadequate, where the market will fail to provide the best outcome. [21]

Dealing with market failure is politically challenging, as it involves deferring individual interests to the larger societal good. This political difficulty has been true since the earliest days of the republic. Steam engines, although notoriously unsafe, had to wait 40 years until a series of savage accidents costing hundreds of lives led Congress to impose safety regulations. Automobile safety rules took more than half a century and faced strong opposition from manufacturers. Air safety regulations appeared more than 20 years after the first flight. A foundational belief for the United States is that "intellect and practical science," as an early Congressional report explaining why regulation was unnecessary for steamboats stated, will lead to improvement via some automatic and self-correcting market process, without government intervention.[22] The decision of the United States to take a minimalist approach to regulating the internet had considerable influence on other nations. In part, this reflects U.S. diplomatic efforts in multilateral for to win support for policies that emphasized private sector control. These efforts were reinforced by the rapid growth of the U.S. economy in the 1990s.

8.4 Sovereignty and the Illusion of the Commons

The Organization for Economic Co-operation and Development (OECD) defines global commons as natural assets outside national jurisdiction such as the oceans, outer space and the Antarctic.[24] Cyberspace is not a commons. Sovereignty completely covers cyberspace, even if nations have not always chosen to assert sovereign control (and the reasons for this may be a

combination of poorly conceived ideology and concerns over liability and regulation). This is because cyberspace is an artificial creation which rests on a tangible, physical construct. There is no moment when bits moving from one computer to another are not on a network that someone owns and that is physically located in a sovereign state. The exceptions might be undersea cables or satellite trans-missions, but the action still takes place on an owned facility were the owner is subject to some country and its laws. We can show ownership at any moment. Sometimes this is forensically challenging, but there are ways to reduce the forensic challenge to be able to assign sovereign responsibility.

This legal construct accommodates commerce, but it also enables covertness and reinforces deniability. Sovereignty in cyberspace is not ambiguous, but the perception that it is so allows us to evade thorny issues. Western nations, as those currently most vulnerable to cyber attacks and those most constrained by law, might gain more than they would lose by changing these rules to allow nations to close their networks to traffic designed for criminal or offensive purposes. Cyberspace is a "pseudo commons," more like a condominium or a shopping mall. It is a shared global infrastructure. Governance of this infrastructure is both weak and fragmented, but sovereign authority exists, even if it is not usually asserted or enforced. This "passive sovereignty" depends on political decisions by governments not to assert control and instead to rely on commercial agreements that create strong interconnections to provide a governance structure, but this decision could be changed at any time.

However, as new technologies increase the scope for monitoring and intervention in the flow of traffic, and as nations question the "hands-off" approach originally taken by the United States, passive sovereignty is evolving into a more active assertion of the rights of national governments to exert control. Countries are beginning to assert sovereign control over their national cyberspace. The next steps will be to deploy technologies to let them enforce control and to create multilateral governance structures to legitimize these actions.[25]

8.5 Reconsidering the Role of Government

Cyberspace is increasingly Hobbesian, and the belief of the pioneers that a "social con-tract" would emerge naturally from the self-organizing internet community without the intervention of the state has proven to be either

wrong or moving at a pace so slow that threatens security. Beliefs about the nature of cyberspace have downplayed the role of formal governance and governments. Changing this assumption is part of the long-term process to adjust to the new environment created by technological change.

This is not unusual; when new technologies come along, they are either un-regulated or efforts are made to regulate them with the old, antiquated rules. As the technologies mature and governments gain experience with them, they are brought into the ambit of societal control. However, unlike the 1990s, when most internet technology and users came from the United States, this process of reconsideration may now Governments will establish sovereignty in cyberspace, but it is yet an open question as to whether this extension will be consistent with Western values or it will lead to a fragmented, less open internet. Other nations will extend government control in ways that may not be to our liking.[26] A failure to move from the beliefs of the internet pioneers could put democratic values at risk. The benefit of worldwide use of a U.S. internet architecture is that it reflects Western political values, such as openness for ideas and discourse, which are not universally esteemed by all governments. As innovation and manufacturing shift from the U.S. to the Pacific and as the equipment upon which cyberspace rests is built in countries with very different political ideals, we could easily see this openness contract. The result could be a cyberspace that would be open for business, but not to ideas.

The reasons for this are not readily apparent, but those who set the standards, manufacture the hardware and write the code have a deep degree of control. While we debate the size and nature of the global commons, other nations may seize the opportunity to "rearchitect" cyberspace to better serve their political and commercial needs. The U.S. ideology and culture that shaped cyberspace is now subject to subtle changes as manufacturing spreads to Asia and as Americans no longer constitute the largest number of internet users.

The struggles over the Domain Name System (DNS) and ICANN, the battles over technology standards, and the problems at the International Telecommunications Union (ITU) are all symptoms of this reorientation of internet governance to reflect the increasing influence of other nations. Cyberspace is being reshaped. National governments, with all their resources and power, have entered cyberspace and we cannot dismiss their efforts to reshape the domain for economic and political advantage. Perhaps the United States still has enough influence to put forward a new vision for cyberspace to make it more secure and yet still amenable to our political values. Doing this

will require rethinking the role of government and recognizing the scope of sovereignty. All of this leads us to the antithesis of the original view of the role of government in cyberspace. In this new phase of administering and securing the internet, governments

8.6 References

1. Ira Magaziner, "Democracy and Cyberspace: First Principles," presented at the conference on Democracy and Digital Media, Massachusetts Institute of Technology, Cambridge, 8 May 1998.
2. Telecom deregulation, however, is an inadequate model for the Internet, as it is concerned with ownership and the introduction of competition into the supply of telecom services.
3. National Telecommunications and Information Agency, "Statement of Policy, Management of Internet Names and Addresses," 1998, http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm.
4. The most famous example is Gilder's Declaration of Independence.
5. A government designed encryption module that could be inserted into computers and other network devices that made data inaccessible to all but Federal authorities.
6. The author was a member of the security group.
7. Organization for Economic Cooperation and Development, "The Future of the Internet Economy," OECD (June 2008), http://www.oecd.org/dataoecd/20/41/40789235.pdf.
8. S. Bellovin, D. Clark, A Perrig, D. Song:,"A Clean-Slate Design for the Next-Generation Secure Internet," National Science Foundation (2005): 2, http://www.nsf.gov/cise/cns/geni/ngsi.pdf.
9. John Barlow, "A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/~barlow/Declaration-Final.html.
10. Protocols, contracts and national laws that determine what actions form the architecture of cyber-space and what relationships are permissible.
11. William Nordhaus, "Paul Samuelson and Global Public Goods," Yale University (May 2005) http://nordhaus.econ.yale.edu/PASandGPG.pdf.
12. Top Ten Buzzwords, http://www.cnet.com/1990-11136_1-6275610-1.html.
13. Howard Rheingold, "Chapter Two: Daily Life in Cyberspace: How the Computerized Counterculture Built a New Kind of Place,"

http://www.rheingold.com/vc/book/2.html.
14. Kevin Kelly (who went on to found *Wired* and who preceded Rheingold as an editor of the *Whole Earth Catalogue*), *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*

16.7 Check your progress

1. The term criminal law means crimes that may establish _____.
2. In India Cyber Defamation results in _____ as well as _____ proceedings against the accused.
3. Crime is a _____and _____ phenomenon and is as old as the human society.
4. Computer forensic cells CFSLs refers to _____ .
5. CrPC describe itself as _____ .

16.8 Answers to check your progress

1. Punishments
2. Civil/ Criminal
3. Social/ economic
4. Central Forensic Laboratories
5. Code of Criminal Procedure

16.9 Terminal Questions

1. How cyber defamation affects in corporate world?
2. Explain the procedure of blocking of content?
3. In Indian regulations, blocking of website or deletion of content is described under which law. Discuss.
4. Explain any two cases related to online defamation?
5. How would you describe defamation and cyber defamation separately?

Unit-9
Cyber Space and Freedom of Speech and Expression

Objectives:

After going through this unit you should be able to:

- Understand the legal regime of social media and freedom of expression.
- Understand the constitutional validity of 66A of IT act, 2000.
- Understand the phenomenon between rights and responsibilities.

Structure

9.1 Introduction[35]

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.

[35]The Law, Social Media and Freedom of Speech by Internet Rights; retrieved from http://internetrights.in/programs/internet-governance/the-law-social-media-and-freedom-of-speech/

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 Centre) before making any arrest," a bench of justices B S Chauhan and Dipak Misra said.

9.2 Constitutional validity of section 66A of IT Act[36]

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 of 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))

[36]The Law, Social Media and Freedom of Speech by Internet Rights; retrieved from http://internetrights.in/programs/internet-governance/the-law-social-media-and-freedom-of-speech/

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 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.

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 Rs. 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 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 criminalized (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 criminalizing 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.[37]

9.3 Criminalization of Online Speech and Social Media[38]

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.

[37] Breaking Down Section 66A of the IT Act by The Centre For Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act

[38] India: Digital freedom under threat? Criminalization of online speech by Melody Patry, 21 November, 2013; retrieved from http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-2/

9.4 Recent Cases[39]

The petition was also filed regarding the arrest of a Hyderabad-based woman activist, who was sent to jail over her Face book 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.

9.5 Case study: Face book arrests[40]

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

[39]The Law, Social Media and Freedom of Speech by Internet Rights; retrieved from http://internetrights.in/programs/internet-governance/the-law-social-media-and-freedom-of-speech/

[40]India: Digital freedom under threat? Criminalization of online speech by Melody Patry, 21 November, 2013; retrieved from http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-2/

"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 Rs. 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.

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.[41]

9.6 Rights vs. Responsibilities[42]

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 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

[41] Social Media Regulation vs. Suppression of Freedom of Speech by Pranesh Prakash, November 19, 2012; retrieved from http://kafila.org/2012/11/19/social-media-regulation-vs-suppression-of-freedom-of-speech-pranesh-prakash/

[42] The Law, Social Media and Freedom of Speech by Internet Rights; retrieved from http://internetrights.in/programs/internet-governance/the-law-social-media-and-freedom-of-speech/

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 Face book, 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, 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, defense 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 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. 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 organizations, 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.[43]

9.7 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

[43] Regulating social media or reforming section 66A? Our recommendations to the Law Commission of India by Anja Kovacs; retrieved from http://internetdemocracy.in/reports/regulating-social-media-or-reforming-section-66a-our-recommendations-to-the-law-commission-of-india/

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.

9.8 Summary

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.

9.9 References

1. The Law, Social Media and Freedom of Speech by Internet Rights; retrieved from http://internetrights.in/programs/internet-governance/the-law-social-media-and-freedom-of-speech/
2. Breaking Down Section 66A of the IT Act by The Centre For Internet & Society; retrieved from http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act
3. India: Digital freedom under threat? Criminalization of online speech by Melody Patry, 21 November, 2013; retrieved from http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-2/
4. Social Media Regulation vs. Suppression of Freedom of Speech by Pranesh Prakash, November 19, 2012; retrieved from http://kafila.org/2012/11/19/social-media-regulation-vs-suppression-of-freedom-of-speech-pranesh-prakash/
5. Regulating social media or reforming section 66A? Our recommendations to the Law Commission of India by Anja Kovacs; retrieved from http://internetdemocracy.in/reports/regulating-social-media-or-reforming-section-66a-our-recommendations-to-the-law-commission-of-india/

9.10 Check your progress

1) Section 66A punishes persons for sending _____.

2) The current equivalent laws in the UK are the _____ Act, 2003.
3) _____ of the IT Act is both overly broad and also carries a disproportionate punishment.
4) The provision carries a penalty of up to _____ imprisonment and a fine.
5) _____ needs to be promoted with legitimate limitations and in balance with other digital rights within an expanded legal and regulatory framework.

9.11 Answers to check your progress

1) Offensive messages
2) Communications
3) Section 66A
4) Three years
5) Freedom of expression

9.12 Terminal Questions

1) Explain difference between rights and responsibilities?
2) Discuss some consequences of section 66A.
3) What do you understand by sending and publishing?
4) Discuss Facebook case study of Shaheen Dhada.
5) How freedom of speech and expression performs in social media?

Unit-10

Software Development and Legal Issues

OBJECTIVES

After going through this unit you should be able to:

- Understanding the meaning of cyber forensics and objectives behind it.
- Understanding the legal perspectives for cyber forensics.
- Understanding the phases of cybercrime with relevant case study.

Structure

10.1 Introduction

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.

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.[44]

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. [45]
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 checksums 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

[44] An investigation of Computer Forensics by Ryan Pidanick; retrieved from http://www.isaca.org/Journal/Past-Issues/2004/Volume-3/Pages/An-Investigation-of-Computer-Forensics.aspx

[45]Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf

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.[46]

10.2 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."[47]

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."[48]

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." [49]

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

[46]Issues in Computer Forensics (.pdf) by Sonia Bui et. al; retrieved from http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf

[47]Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf

[48]Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf

[49]Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf

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.

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.[50]

10.3 Objectives of Cyber Forensics[51]

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

10.4 Legal Scenario[52]

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

[50]Computer forensics (cyber forensics) by Margaret Rouse; retrieved from http://searchsecurity.techtarget.com/definition/computer-forensics

[51]Plethora of Cyber Forensics by N. Sridhar, et. al.; retrieved from http://thesai.org/Downloads/Volume2No11/Paper%2018-%20Plethora%20of%20Cyber%20Forensics.pdf

[52] The challenges facing computer forensics investigators in obtaining information form mobile devices for use in criminal investigations by David W. Bennett; retrieved from http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

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 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.

10.5 Legal Provisions in Indian Perspective[53]

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 facie acceptability of digital evidence in any trial.

[53]Cyber Forensics: law and practice in India | iPleaders http://blog.ipleaders.in/cyber-forensics-law-and-practice-in-india/#ixzz3FpZ7Gmxg

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.

10.6 Phases of Cyber Forensics[54]

10.6.1 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 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

[54]Plethora of Cyber Forensics by N. Sridhar, et. al.; retrieved from http://thesai.org/Downloads/Volume2No11/Paper%2018-%20Plethora%20of%20Cyber%20Forensics.pdf

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.

10.6.2 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.

10.6.3 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.

10.6.4 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.

10.7 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.

10.8 Cyber Forensic Tools[55]

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.

[55]Plethora of Cyber Forensics by N. Sridhar, et. al.; retrieved from http://thesai.org/Downloads/Volume2No11/Paper%2018-%20Plethora%20of%20Cyber%20Forensics.pdf

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.

10.9 Case Laws

State of Maharashtra vs. Dr. Praful B Desai (AIR 2003 SC 2053)[56]

[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[57]

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.

[56]Electronic Evidence and Cyber Law by Adv. Prashant Mali; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a

[57] Cyber Forensics in India; retrieved from http://perry4law.org/cfii/

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)[58]

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.

10.10 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 organizations now look to the experts to uncover this evidence discreetly and without disrupting business continuity.

10.11 Summary

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

[58]Electronic Evidence and Cyber Law by Adv. Prashant Mali; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a

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.

10.12 References

1) An investigation of Computer Forensics by Ryan Pidanick; retrieved from http://www.isaca.org/Journal/Past-Issues/2004/Volume-3/Pages/An-Investigation-of-Computer-Forensics.aspx
2) Computer Forensics: Bringing the Evidence to Court by Cornell Walker; retrieved from
i. http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf
3) Issues in Computer Forensics (.pdf) by Sonia Bui et. al; retrieved from http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf
4) Computer forensics (cyber forensics) by Margaret Rouse; retrieved from http://searchsecurity.techtarget.com/definition/computer-forensics
5) Plethora of Cyber Forensics by N. Sridhar, et. al.; retrieved from http://thesai.org/Downloads/Volume2No11/Paper%2018-%20Plethora%20of%20Cyber%20Forensics.pdf
6) The challenges facing computer forensics investigators in obtaining information form mobile devices for use in criminal investigations by David W. Bennett; retrieved from http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/
7) Cyber Forensics: law and practice in India | iPleaders http://blog.ipleaders.in/cyber-forensics-law-and-practice-in-india/#ixzz3FpZ7Gmxg
8) Electronic Evidence and Cyber Law by Adv. Prashant Mali; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a
9) Cyber Forensics in India; retrieved from http://perry4law.org/cfii/

10.13 Check your progress

1) The _____ is the process of identifying evidence material and its probable location.
2) The _____ saves the state of evidence that can be further analyzed.
3) The analysis phase collects the _____ and examines it to find the pieces of evidences.
4) The reporting phase comprises of _____ and _____ retention.
5) The main objective of _____ is to extract digital evidence which can be admissible in court of law.

10.14 Answers to check your progress

1) Identification phase
2) Acquisition phase
3) Acquired data
4) Documentation and evidence
5) Cyber forensics tools

10.15 Terminal questions

1) Explain the concept of cyber forensic tools with example?
2) Discuss different phases of cyber forensics.
3) What are the objectives of cyber forensics?
4) Describe the forensics methodology in digital world.
5) What are the legal regulations mentioned in cyber forensics?

Unit-11
Licensing Agreement with Reference to International Treaties

Objectives:

This unit has been prepared to acquaint you with

- What are licensing agreements;
- How they are governed by International treaties.

Structure

11.1 Introduction

1) During the last century, before the existence of any international convention in the field of industrial property, it was difficult to obtain protection for industrial property rights in the various countries of the world because of the diversity of their laws. Moreover, patent applications had to be made roughly at the same time in all countries in order to avoid a publication in one country destroying the novelty of the invention in the other countries. These practical problems

created a strong desire to overcome such difficulties.

2) During the second half of the last century the development of a more internationally oriented flow of technology and the increase of international trade made harmonization of industrial property laws urgent in both the patent and the trademark field.

3) When the Government of the Empire of Austria-Hungary invited the other countries to participate in an international exhibition of inventions held in 1873 at Vienna, participation was hampered by the fact that many foreign visitors were not willing to exhibit their inventions at that exhibition in view of the inadequate legal protection offered to exhibited inventions.
4) This led to two developments: firstly, a special Austrian law secured temporary protection to all foreigners participating in the exhibition for their inventions, trademarks and industrial designs. Secondly, the Congress of Vienna for Patent Reform was convened during the same year, 1873. It elaborated a number of principles on which an effective and useful patent system should be based, and urged governments "to bring about an international understanding upon patent protection as soon as possible."
5) As a follow-up to the Vienna Congress, an International Congress on Industrial Property was convened at Paris in 1878. Its main result was a decision that one of the governments should be asked to convene an international diplomatic conference "with the task of determining the basis of uniform legislation" in the field of industrial property.
6) Following that Congress, a final draft proposing an international "union" for the protection of industrial property was prepared in France and was sent by the French Government to a number of other countries, together with an invitation to attend the 1880 International Conference in Paris. That Conference adopted a draft convention which contained in essence the substantive provisions that today are still the main features of the Paris Convention.
7) A Diplomatic Conference was convened in Paris in 1883, which ended with final approval and signature of the Paris Convention for the Protection of Industrial Property. The Paris Convention was signed by 11 States: Belgium, Brazil, El Salvador, France, Guatemala, Italy, the Netherlands, Portugal, Serbia, Spain and Switzerland. When it came into effect on July 7, 1884, Great Britain, Tunisia and Ecuador had adhered as well, bringing the initial number of member countries to 14. El Salvador, Guatemala and Ecuador later denounced the Paris Convention to join again in the 1990s. It was only during

the first quarter of the 20th century and then particularly after World War II that the Paris Convention increased its membership more significantly.

8) The Paris Convention has been revised from time to time after its signature in 1883. Each of the revision conferences, starting with the Brussels Conference in 1900, ended with the adoption of a revised Act of the Paris Convention. With the exception of the Acts concluded at the revision conferences of Brussels (1897 and 1900) and Washington, D.C. (1911), which are no longer in force, all those earlier Acts are still of significance, although the great majority of the countries are now party to the latest Act, that of Stockholm of 1967.

11.2 Principal Provisions

The provisions of the Paris Convention may be sub-divided into four main categories:

- a first category contains rules of substantive law which guarantee a basic right known as the right to national treatment in each of the member countries;
- a second category establishes another basic right known as the right of priority;
- a third category defines a certain number of common rules in the field of substantive law which contain either rules establishing rights and obligations of natural persons and legal entities, or rules requiring or permitting the member countries to enact legislation following those rules;
- a fourth category deals with the administrative framework which has been set up to implement the Convention, and includes the final clauses of the Convention.

11.3 National Treatment

1) National treatment means that, as regards the protection of industrial property, each country party to the Paris Convention must grant the same protection to nationals of the other member countries as it grants to its own nationals. The relevant provisions are contained in Articles 2 and 3 of the Convention.
2) The same national treatment must be granted to nationals of countries which are not party to the Paris Convention if they are domiciled in a member country or if they have a “real and effective” industrial or commercial establishment in such a country. However, no requirement as to domicile or establishment in the country where protection is claimed may be imposed upon nationals of member

countries as a condition for benefiting from an industrial property right.

3) This national treatment rule guarantees not only that foreigners will be protected, but also that they will not be discriminated against in any way. Without this, it would frequently be very difficult and sometimes even impossible to obtain adequate protection in foreign countries for inventions, trademarks and other subjects of industrial property.

The national treatment rule applies first of all to the "nationals" of the member countries. The term "national" includes both natural persons and legal entities. With respect to legal entities, the status of being a national of a particular country may be difficult to determine. Generally, no nationality as such is granted to legal entities by the various national laws. There is of course no doubt that State-owned enterprises of a member country or other entities created under the public law of such country are to be considered as nationals of the member country concerned. Legal entities created under the private law of a member country will usually be considered a national of that country. If they have their actual headquarters in another member country, they may also be considered a national of the headquarters country. According to Article 2(1), the national treatment rule applies to all advantages that the various national laws grant to nationals.

1) This means furthermore, that any requirement of reciprocity of protection is excluded. Supposing that a given member country has a longer term of patent protection than another member country: the former country will not have the right to provide that nationals of the latter country will enjoy a term of protection of the same length as the term of protection is in the law of their own country. This principle applies not only to codified law but also to the practice of the courts (jurisprudence), and to the practice of the Patent Office or other administrative governmental institutions as it is applied to the nationals of the country.

2) The application of the national law to the national of another member country does not, however, prevent him from invoking more beneficial rights specially provided in the Paris Convention. These rights are expressly reserved. The national treatment principle must be applied without prejudice to such rights.

3) Article 2(3) states an exception to the national treatment rule. The national law relating to judicial and administrative procedure, to jurisdiction and to requirements of representation is expressly "reserved." This means that certain requirements of a mere procedural nature which impose special conditions on

foreigners for purposes of judicial and administrative procedure, may also validly be invoked against foreigners who are nationals of member countries. An example is a requirement for foreigners to deposit a certain sum as security or bail for the costs of litigation. Another example is expressly stated: the requirement that foreigners should either designate an address for service or appoint an agent in the country in which protection is requested. This latter is perhaps the most common special requirement imposed on foreigners.

4) Article 3 provides for the application of the national treatment rule also to nationals of non-member countries, if they are *domiciled* or have an industrial or commercial establishment in a member country.

5) The term "domiciled" is generally interpreted not only in the strict legal sense of the term. A mere residence, more or less permanent as distinct from a legal domicile, is sufficient. Legal entities are domiciled at the place of their actual headquarters.

6) If there is no domicile, there may still be an industrial or commercial establishment which gives a person the right to national treatment. The notion of the industrial or commercial establishment in a member country of a national of a non-member country is further qualified by the text of the Convention itself. It requires that there must be actual industrial or commercial activity. A mere letter box or the renting of a small office with no real activity is not sufficient.

11.4 The Right of Priority

The right of priority means that, on the basis of a regular application for an industrial property right filed by a given applicant in one of the member countries, the same applicant (or its or his successor in title) may, within a specified period of time (six or 12 months), apply for protection in all the other member countries. These later applications will then be regarded as if they had been filed on the same day as the earliest application. Hence, these later applications enjoy a priority status with respect to all applications relating to the same invention filed after the date of the first application. They also enjoy a priority status with respect to all acts accomplished after that date which would normally be apt to destroy the rights of the applicant or the patentability of his invention. The provisions concerning the right of priority are contained in Article 4 of the Convention.

The right of priority offers great practical advantages to the applicant desiring protection in several countries. The applicant is not required to present all

applications at home and in foreign countries at the same time, since he has six or 12 months at his disposal to decide in which countries to request protection. The applicant can use that period to organize the steps to be taken to secure protection in the various countries of interest in the particular case.

1) The beneficiary of the right of priority is any person entitled to benefit from the national treatment rule who has duly filed an application for a patent for invention or another industrial property right in one of the member countries.

2) The right of priority can be based only on the *first* application for the same industrial property right which must have been filed in a member country. It is therefore not possible to follow a first application by a second, possibly improved application and then to use that second application as a basis of priority. The reason for this rule is obvious: one cannot permit an endless chain of successive claims of priority for the same subject, as this could, in fact, considerably prolong the term of protection for that subject.

3) Article 4A(l) of the Paris Convention recognizes expressly that the right of priority may also be invoked by the successor in title of the first applicant. The right of priority may be transferred to a successor in title without transferring at the same time the first application itself. This allows in particular also the transfer of the right of priority to different persons for different countries, a practice which is quite common.

4) The later application must concern the same subject as the first application the priority of which is claimed. In other words, the same invention, utility model, trademark or industrial design must be the subject of both applications. It is, however, possible to use a first application for a patent for invention as priority basis for a registration of a utility model and vice versa. The same change of form of protection in both directions may also be possible, in accordance with national laws, between utility models and industrial designs.

5) The first application must be "duly filed" in order to give rise to the right of priority. Any filing, which is equivalent to a regular national filing, is a valid basis for the right of priority. A regular national filing means any filing that is adequate to establish the date on which the application was filed in the country concerned. The notion of "national" filing is qualified by including also applications filed under bilateral or multilateral treaties concluded between member countries.

6) Withdrawal, abandonment or rejection of the first application does not destroy its capacity to serve as a priority basis. The right of priority subsists

even where the first application generating that right is no longer existent.

7) The effect of the right of priority is regulated in Article 4B. One can summarize this effect by saying that, as a consequence of the priority claim, the later application must be treated as if it had been filed already at the time of the filing, in another member country, of the first application the priority of which is claimed. By virtue of the right of priority, all the acts accomplished during the time between the filing dates of the first and the later applications, the so-called priority period, cannot destroy the rights which are the subject of the later application.

8) In terms of concrete examples, this means that a patent application for the same invention filed by a third party during the priority period will not give a prior right, although it was filed before the later application. Likewise, a publication or public use of the invention, which is the subject of the later application, during the priority period would not destroy the novelty or inventive character of that invention. It is insignificant for that purpose whether that publication is made by the applicant or the inventor himself or by a third party.

9) The length of the priority period is different according to the various kinds of industrial property rights. For patents for invention and utility models the priority period is 12 months, for industrial designs and trademarks it is six months. In determining the length of the priority period, the Paris Convention had to take into account the conflicting interests of the applicant and of third parties. The priority periods now prescribed by the Paris Convention seem to strike an adequate balance between them.

10) The right of priority as recognized by the Convention permits the claiming of "multiple priorities" and of "partial priorities." Therefore, the later application may not only claim the priority of one earlier application, but it may also combine the priority of several earlier applications, each of which pertaining to different features of the subject matter of the later application. Furthermore, in the later application, elements for which priority is claimed may be combined with elements for which no priority is claimed. In all these cases, the later application must of course comply with the requirement of unity of invention.

11) These possibilities correspond to a practical need. Frequently after a first filing further improvements and additions to the invention are the subject of further applications in the country of origin. In such cases, it is very practical to

be able to combine these various earlier applications into one later application, when filing before the end of the priority year in another member country. This combination is even possible if the multiple priorities come from different member countries.

11.5 Provisions Concerning Patents

Independence of Patents

1) Patents for invention granted in member countries to nationals or residents of member countries must be treated as independent of patents for invention obtained for the same invention in other countries, including non-member countries. The rule concerning the "independence" of patents for invention is contained in Article 4*bis*.

2) This principle is to be understood in its broadest sense. It means that the grant of a patent for invention in one country for a given invention does not oblige any other member country to grant a patent for invention for the same invention. Furthermore, the principle means that a patent for invention cannot be refused, invalidated or otherwise terminated in any member country on the ground that a patent for invention for the same invention has been refused or invalidated, or that it is no longer maintained or has terminated, in any other country. In this respect, the fate of a particular patent for invention in any given country has no influence whatsoever on the fate of a patent for the same invention in any of the other countries.

3) The underlying reason and main argument in favor of this principle is that national laws and administrative practices are usually quite different from country to country. A decision not to grant or to invalidate a patent for invention in a particular country on the basis of its law will frequently not have any bearing on the different legal situation in the other countries. It would not be justified to make the owner lose the patent for invention in other countries, on the ground that he or she lost a patent in a given country as a consequence of not having paid an annual fee in that country, or as a consequence of the patent's invalidation in that country, on a ground which does not exist in the laws of the other countries.

4) A special feature of the principle of independence of patents for invention is contained in Article 4*bis*(5). This provision requires that a patent granted on an application which claimed the priority of one or more foreign applications, must be given the same duration which it would have according to the national law if no priority had been claimed. In other words, it is not permitted to deduct

the priority period from the term of a patent invoking the priority of a first application. For instance, a provision in a national law starting the term of the patent for invention from the (foreign) priority date, and not from the filing date of the application in the country, would be in violation of this rule.

11.6 The Right of the Inventor to be Mentioned

1) A general rule states that the inventor must have the right to be mentioned as such in the patent for invention. This is stated in Article 4*ter*.
2) National laws have implemented this provision in several ways. Some give the inventor only the right for civil action against the applicant or owner in order to obtain the inclusion of his name in the patent for invention. Others — and that tendency seems to be increasing — enforce the naming of the inventor during the procedure for the grant of a patent for invention on an *ex officio* basis. In the United States of America, for example, it is even required that the applicant for a patent be the inventor himself.

11.7 Importation, Failure to Work and Compulsory Licenses

1) The questions of importation of articles covered by patents, of failure to work the patented invention and of compulsory licenses, are dealt with in Article 5A of the Convention.

2) With respect to importation, the provision states that importation by the patentee, into the country where the patent has been granted, of articles covered by the patent and manufactured in any of the countries of the Union will not entail forfeiture of the patent. This provision is quite narrowly worded, and hence only applies when several conditions are met. Consequently the countries of the Union have considerable leeway to legislate with respect to importation of patented goods under any of the circumstances which are different to those foreseen in this provision.

3) This Article applies to patentees who are entitled to benefit from the Paris Convention and who, having a patent in one of the countries of the Paris Union, import to this country goods (covered by the patent) which were manufactured in another country of the Union. In such a case, the patent granted in the country of importation may not be forfeited as a sanction for such importation. In this context, the term “patentee” would also cover the representative of the patentee, or any person who effects the importation in the name of such

patentee.

4) With respect to the goods that are imported, it suffices that they be manufactured in a country of the Union. The fact that the goods, having been manufactured in a country of the Union, are thereafter circulated through other countries and eventually imported from a country which is not a member of the Union, would not prevent this Article from being applicable.

5) Finally, it may be mentioned that the term "forfeiture" in Article 5A(1) includes any measure which has the effect of definitively terminating the patent. Therefore it would cover the concepts of invalidation, revocation, annulment, repeal, etc. Whether "forfeiture" may, in the light of the purpose of this Article or the spirit of the Paris Convention, be construed as covering also other measures that would have the effect of preventing importation (fines, suspension of rights, etc.) is left for the national legislation and courts to decide.

6) With respect to the working of patents and compulsory licenses, the essence of the provisions contained in Article 5A is that each country may take legislative measures providing for the grant of compulsory licenses. These compulsory licenses are intended to prevent the abuses which might result from the exclusive rights conferred by a patent for invention, for example failure to work or insufficient working.

7) Compulsory licenses on the ground of failure to work or insufficient working are the most common kind of coercive measure against the patent owner to prevent abuses of the rights conferred by the patent for invention. They are expressly dealt with by Article 5A.

8) The main argument for enforcing working of the invention in a particular country is the consideration that, in order to promote the industrialization of the country, patents for invention should not be used merely to block the working of the invention in the country or to monopolize importation of the patented article by the patent owner. They should rather be used to introduce the use of the new technology into the country. Whether the patent owner can really be expected to do so, is first of all an economic consideration and then also a question of time. Working in all countries is generally not economical. Moreover, it is generally recognized that immediate working in all countries is impossible. Article 5A therefore tries to strike a balance between these conflicting interests.

9) Compulsory licenses for failure to work or insufficient working of the invention may not be requested before a certain period of time has elapsed.

This time limit expires either four years from the date of filing of the patent application or three years from the date of the grant of the patent for invention. The applicable time is the one which, in the individual case, expires last.

10) The time limit of three or four years is a minimum time limit. The patent owner must be given a longer time limit, if he can give legitimate reasons for his inaction — for example, that legal, economic or technical obstacles prevent working, or working more intensively, the invention in the country. If that is proven, the request for a compulsory license must be rejected, at least for a certain period. The time limit of three or four years is a minimum also in the sense that national law can provide for a longer time limit.

11) The compulsory license for non-working or insufficient working must be a non-exclusive license and can only be transferred together with the part of the enterprise benefiting from the compulsory license. The patent owner must retain the right to grant other non-exclusive licenses and to work the invention himself. Moreover, as the compulsory license has been granted to a particular enterprise on the basis of its known capacities, it is bound to that enterprise and cannot be transferred separately from that enterprise. These limitations are intended to prevent a compulsory licensee from obtaining a stronger position on the market than is warranted by the purpose of the compulsory license, namely, to ensure sufficient working of the invention in the country.

12) All these special provisions for compulsory licenses in Article 5A(4) are only applicable to compulsory licenses for non-working or insufficient working. They are not applicable to the other types of compulsory licenses for which the national law is free to provide. Such other types may be granted to prevent other abuses, for example, excessive prices or unreasonable terms for contractual licenses or other restrictive measures which hamper industrial development.

13) Compulsory licenses may also be granted for reasons of the public interest, in cases where there is no abuse by the patent owner of his rights — for example, in the fields of military security or public health.

14) There are also cases where a compulsory license is provided for to protect the public interest in unhampered technological progress. This is the case of the compulsory license in favor of the so-called *dependent patents*. If a patented invention cannot be worked without using an earlier patent for invention granted to another person, then the owner of the dependent patent, in certain circumstances, may have the right to request a compulsory license for the use of that invention. If the owner of the dependent patent for invention obtains the

compulsory license, he may in turn be obliged to grant a license to the owner of the earlier patent for invention.

15) All these other types of compulsory licenses can be grouped together under the general heading of compulsory licenses *in the public interest*. National laws are not prevented by the Paris Convention from providing for such compulsory licenses, and they are not subject to the restrictions provided for in Article 5A. This means in particular that compulsory licenses in the public interest can be granted without waiting for the expiration of the time limits provided for compulsory licenses that relate to failure to work or insufficient working.

16) It should be noted, however, that Article 31 of the TRIPS Agreement further provides a number of conditions with respect to the use of subject matter of a patent without the authorization of the right-holder.

17) *Grace Period for the Payment of Maintenance Fees*

18) Article 5*bis* provides for a grace period for the payment of maintenance fees for industrial property rights and deals with the restoration of patents for invention in case of non-payment of fees.

19) In most countries the maintenance of certain industrial property rights, mainly the rights in patents for invention and trademarks, is subject to the periodical payment of fees. For patents, the maintenance fees must generally be paid annually, and in that case are also called annuities. Immediate loss of the patent for invention in the event that one annuity is not paid at the due date would be too harsh a sanction. Therefore, the Paris Convention provides for a period of grace, during which the payment can still be made after the due date to maintain the patent. That period is six months, and is established as a minimum period, leaving countries free to accept a longer period.

20) The delayed payment of the annuity may be subjected to the payment of a surcharge. In that case, both the delayed fee and the surcharge must be paid within the grace period. During the grace period, the patent for invention remains provisionally in force. If the payment is not made during the grace period, the patent for invention will lapse retroactively, that is, as of the original due date of the annuity.

11.8 Patents in International Traffic

1) Another common rule of substantive importance, containing a limitation of the rights of the patent owner in special circumstances, is contained in Article 5*ter*. It deals with the transit of devices on ships, aircraft or land vehicles through a

member country in which such device is patented.

2) Where ships, aircraft or land vehicles of other member countries enter temporarily or accidentally a given member country and have on board devices patented in that country, the owner of the means of transportation is not required to obtain prior approval or a license from the patent owner. Temporary or accidental entry of the patented device into the country in such cases constitutes no infringement of the patent for invention.
3) The device on board the ship, aircraft or vehicle must be in the body, in the machinery, tackle, gear or other accessories of the conveyance, and must be used exclusively for operational needs.
4) The provision covers only the use of patented devices. It does not allow the making of patented devices on board a means of transportation, nor the sale to the public of patented products or of products obtained under a patented process.

Inventions Shown at International Exhibitions

1) A further common rule of a substantive nature is the provision concerning temporary protection in respect of goods exhibited at international exhibitions, contained in Article 11 of the Convention.
2) The principle stated in Article 11 is that the member countries are obliged to grant, in conformity with their domestic legislation, temporary protection to patentable inventions, utility models, industrial designs and trademarks in respect of goods exhibited at official or officially recognized international exhibitions held in the territory of any member country.
3) Temporary protection may be provided by various means. One is to grant a special right of priority, similar to that provided for in Article 4. This priority right would start from the date of the opening of the exhibition or from the date of the introduction of the object at the exhibition. It would be maintained for a certain period from that date, say 12 months, and would expire if the application for protection does not follow the exhibition within that period.
4) Another means which is found in a number of national laws, in particular with respect to patents for invention, is that of prescribing that, during a certain period of, say, twelve months before the filing or priority date of a patent application, a display of the invention at an international exhibition will not destroy the novelty of the invention. When choosing that solution, it is important to protect the inventor or other owner of the invention during the same period also against abusive acts of third parties. This means in particular that the person exhibiting the invention must be protected against any copying

or usurpation of the invention for purposes of a patent application by a third party. The owner of the invention must also be protected against disclosure, based on the exhibition, by third parties.

5) Article 11 applies only to official or officially recognized exhibitions. The interpretation of that term is left to the member country where protection is sought. An interpretation corresponding to the spirit of Article 11 is to consider an exhibition "official" if it is organized by a State or other public authority, to consider it "officially recognized" if it is not official but has at least been recognized as official by a State or other public authority, and to consider it "international" if goods from various countries are exhibited.

Provisions Concerning Trademarks

Use of Trademarks

1) The Convention touches on the issue of the use of marks in Article 5C(1), (2) and (3).
2) Article 5C(1) relates to the compulsory use of registered trademarks. Some of the countries which provide for the registration of trademarks also require that the trademark, once registered, be used within a certain period. If this use is not complied with, the trademark may be expunged from the register. For this purpose, "use" is generally understood as meaning the sale of good bearing the trademark, although national legislation may regulate more broadly the manner in which use of the trademark is to be complied with. The Article states that where compulsory use is required, the trademark's registration may be cancelled for failure to use the trademark only after a reasonable period has elapsed, and then only if the owner does not justify such failure.
3) The definition of what is meant by "reasonable period" is left to the national legislation of the countries concerned, or otherwise to the authorities competent for resolving such cases. This reasonable period is intended to give the owner of the mark enough time and opportunity to arrange for its proper use, considering that in many cases the owner has to use his mark in several countries.
4) The trademark owner's justification of non-use would be acceptable if it were based on legal or economic circumstances beyond the owner's control, for example if importation of the marked goods had been prohibited or delayed by governmental regulations.
5) The Convention also establishes in Article 5C(2) that the use of a trademark by its proprietor, in a form differing in elements which do not alter the distinctive

character of the mark as it was when formerly registered in one of the countries of the Union, shall not entail invalidation of the registration nor diminish the protection granted to the mark. The purpose of this provision is to allow for unessential differences between the form of the mark as it is registered and the form in which it is used, for example in cases of adaptation or translation of certain elements for such use. This rule applies also to differences in the form of the mark as used in the country of its original registration.

6) Whether in a given case the differences between the mark as registered and the mark as actually used alter the distinctive character is a matter to be decided by the competent national authorities.

Concurrent Use of the Same Trademark by Different Enterprises

1) Article 5C(3) of the Convention deals with the case where the same mark is used for identical or similar goods by two or more establishments considered as co-proprietors of the trademark. It is provided that such concurrent use will not impede the registration of the trademark nor diminish the protection in any country of the Union, except where the said use results in misleading the public or is contrary to the public interest. Such cases could occur if the concurrent use misleads the public as to the origin or source of the goods sold under the same trademark, or if the quality of such goods differs to the point where it may be contrary to the public interest to allow the continuation of such use.

2) This provision does not, however, cover the case of concurrent use of the mark by enterprises which are not co-proprietors of the mark, for instance when use is made concurrently by the owner and a licensee or a franchisee. These cases are left for the national legislation of the various countries to regulate.

Grace Period for the Payment of Renewal Fees

1) Article 5*bis* requires that a period of grace be allowed for the payment of fees due for the maintenance of industrial property rights. In the case of trademarks this provision concerns primarily the payment of renewal fees, since it is by renewal that trademark registrations (and hence the rights that depend on such registrations) may be maintained. A failure to renew the registration will normally entail the lapse of the registration, and in some cases the expiration of the right to the mark. The period of grace provided by the Convention is intended to diminish the risks of a mark being lost by an involuntary delay in the payment of the renewal fees.

2) The countries of the Paris Union are obliged to accord a period of grace of at least six months for the payment of the renewal fees, but are free to provide for the payment of a surcharge when such renewal fees are paid within the period of grace. Moreover, the countries are free to provide for a period of grace longer than the minimum six months prescribed by the Convention.
3) During the period of grace, the registration remains provisionally in force. If the payment of the renewal fees (and surcharge where appropriate) is not made during the period of grace, the registration will lapse with retroactive effect to the original date of expiration.

Independence of Trademarks

1) Article 6 of the Convention establishes the important principle of the independence of trademarks in the different countries of the Union, and in particular the independence of trademarks filed or registered in the country of origin from those filed or registered in other countries of the Union.
2) The first part of Article 6 states the application of the basic principle of national treatment to the filing and registration of marks in the countries of the Union. Regardless of the origin of the mark whose registration is sought, a country of the Union may apply only its domestic legislation when determining the conditions for the filing and registration of the mark. The application of the principle of national treatment asserts the rule of independence of marks, since their registration and maintenance will depend only on each domestic law.
3) This Article also provides that an application for the registration of a mark, filed in any country of the Union by a person who is entitled to the benefits of the Convention, may not be refused, nor may a registration be canceled, on the ground that filing, registration or renewal of the mark has not been effected in the country of origin. This provision lays down the express rule that obtaining and maintaining a trademark registration in any country of the Union may not be made dependent on the application, registration or renewal of the same mark in the country of origin of the mark. Therefore no action with respect to the mark in the country of origin may be required as a prerequisite for obtaining a registration of the mark in that country.

   Finally, Article 6 states that a mark duly registered in a country of the Union shall be regarded as independent of marks registered in the other countries of the Union, including the country of origin. This means that a mark once registered will not be automatically affected by any decision taken with respect to similar registrations for the same marks in other countries. In this respect, the

fact that one or more such similar registrations are, for example, renounced, cancelled or abandoned will not, *eo ipso,* affect the registrations of the mark in other countries. The validity of these registrations will depend only on the provisions applicable in accordance with the legislation of each of the countries concerned.

11.9 Misuse of technology

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.

11.10 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 (Apac) 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.[59]

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,

[59] Cyber defamation increasing in India, The Times of India; retrieved from http://timesofindia.indiatimes.com/tech/it-services/Cyber-defamation-increasing-in-India/articleshow/7122938.cms

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.[60]

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.[61]

11.11 References

1. Cyber and Online Defamation by Pennstate, retrieved from https://wikispaces.psu.edu/display/IST432TEAM4/Cyber+and+Online+Defamation#
2. Online Defamation: A comparative analysis and evaluating the responsibility of the internet service providers in the Indian Legal Frameworks by Abhilasha (JurisOnline.in), retrieved from http://jurisonline.in/?p=2394
3. Cyber defamation increasing in India, The Times of India; retrieved from http://timesofindia.indiatimes.com/tech/it-services/Cyber-defamation-increasing-in-India/articleshow/7122938.cms

[60] Online Defamation: A comparative analysis and evaluating the responsibility of the internet service providers in the Indian Legal Frameworks by Abhilasha (JurisOnline.in), retrieved from http://jurisonline.in/?p=2394

[61] India: Cyber Defamation In Corporate World by Pradhumna Didwania; retrieved from http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+World

4. India: Cyber Defamation In Corporate World by Pradhumna Didwania; retrieved from http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+World

11.12 Check your progress

1. _____ is a statement that harms the reputation of someone else.
2. A _____ is defined as a person or organization who in some way manages the publication/distribution of material online.
3. _____ 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."
4. Cyber defamation attacks and their counter defences assume paramount importance in today's fragile _____ age.
5. _____is a growing tool in brand wars in the business world.

11.13 Answers to check your progress

1. Introduction
2. Provisions process

11.14 Terminal Questions

1. What do you understand by international traffic?
2. What do you mean by national treatment?

Unit-12
Cyber Contract and Information Technology Act, 2000

OBJECTIVES

After going through this unit you should be able to understand:

- the kinds of cybercrime.
- how to tackle cybercrime?
- the major threats and impact of cybercrime.
- the Information Technology Act,2000 and its relation with them.

Structure

12.1 Introduction: 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.

12.2 Categories of Cyber Crime

Cybercrimes are broadly categorized into three categories, namely crime against

12.2.1 Individual

12.2.2 Property

12.2.3 Government

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

12.2.1 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.

12.2.2 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.

12.2.3 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.[62]

[62] Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/

12.3 Different Kinds of Cyber Crime[63]

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 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.[64]

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)[65].

2. **Web Hijacking**

[63] Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

[64] Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

[65] Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

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.
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.

12.4 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.

12.5 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.

12.6 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.

12.7 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 Rs. 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.

1) **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.

2) **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.

3) 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.[66]

4) Email spoofing[67]

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.

5) 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.

6. 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.

---

[66] Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

[67] Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6

7. Theft of information contained in electronic form

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

8. 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.

9. Internet time theft

Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

10. 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.

11. Physically damaging a computer system

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

12. 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.

13. 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.

14. 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.

15. 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.[68]

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.
- 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.

12.8 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

[68] Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

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.[69]

12.9 Major Threats of Cyber Crime in the Current Scenario[70]

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.

12.10 Impact of Cyber Crime on Businesses[71]

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

[69] Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/

[70] Cyber Crime- A Threat to Persons, Property, Government and Societies by Er. Harpreet Singh Dalla et. al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013; retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

[71] Cyber Crime- A Threat to Persons, Property, Government and Societies by Er. Harpreet Singh Dalla et. al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013; retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

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.

12.11 Cyber laws[72]

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

[72] Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Act

12.12 Prevention of Cyber Crime[73]

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.

[73]Cyber Crime- A Threat to Persons, Property, Government and Societies by Er. Harpreet Singh Dalla et. al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013; retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

- 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.

12.13 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. Unlike the later cybercrimes which threaten the very credibility of the internet, cyber pornography promotes the misuse of the internet. Cyber obscenity or pornography is a threat to the netizens. 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.

12.14 Summary

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.

Computer-mediated activities falling within the scope of cyber-pornography/obscenity can be either explicitly prohibited by the law or deemed deviant, namely objectionable because they breach social norms without automatically attracting criminal sanctions. While the debate surrounding this category is complicated by the fact that not all kinds of pornography are illegal, the primary focus of this paper is directed first, towards online representations of sexual deviance, such as indecent images of children circulated via

pedophilias networks; and second, towards activities that carry formal legal sanctions and can be classified as cybercrime either in a broad sense.

12.15 References

1. Cross Domain Solutions: Ensuring Complete Data Security; retrieved from http://www.crossdomainsolutions.com/cyber-crime/
2. Helpline Law: Legal Solutions Worldwide; retrieved from http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html
3. Cyber Crimes: Law and Practice; retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
4. Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csi india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6
5. Cyber Crime- A Threat to Persons, Property, Government and Societies by Er. Harpreet Singh Dallaet. al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013; retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

12.16 Check your progress

1. _____ means repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services.
2. _____ means showing sexual acts in order to cause sexual excitement.
3. Crimes against a government are referred to as _____.
4. Hacking means _____ into a computer system and/or network.
5. _____ refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
6. _____ is rampant within society.
7. The growth of technology has also increased the devastating growth of _____.
8. _____ is a process by which the origin of illegal earnings is disguised.
9. _____ of the Japanese Penal Code forbids the printed portrayal of adult genitals, intercourse and pubic hair.

10. In _____, three States have introduced bills to censor material on the Internet.

12.17 Answers to check your progress

1. Cyber stalking
2. Pornography
3. Cyber terrorism
4. Illegal intrusion
5. Software piracy
6. Pornography
7. Child pornography
8. Money laundering
9. Article 175
10. Australia

12.18 Terminal Questions

1. Explain different categories of cybercrime?
2. Describe cyber stalking and cyber defamation in brief.
3. Discuss 5 kinds of cybercrime.
4. What are the major threats occur in cyber world?
5. How cybercrimes are tackling in upcoming scenario?
6. What do you mean by pedophiles?
7. What is the difference between obscenity and pornography?
8. How money laundering activities relates with pornography?
9. Discuss any two case laws of pornography.
10. Describe some legal regulations applicable in the matter of pornography.

Unit-13

Indian Law and Shrink Wrap Contract

Objectives:

This unit has been prepared to acquaint you with

- What is Shrink Wrap contracts;
- How they are governed;
- How misuse of technology in the form of shrink wrap contract is done etc.

Structure

13.1 Introduction

Shrink-wrap contracts are legal agreements which you are tricked into "signing" without reading, or you are in effect forced to sign because of the situation. This type of thing is very dodgy. Shrink-wrap contracts can be explicit or implicit. Anyway, why is it called a "Shrink-wrap Contract"? I'll explain by way of an example:

Suppose you bought software disc in a shop and you took it home, you might reasonably expect to be able to use it. However, upon examining the packaging, you notice the disc is wrapped in shrink- wrap plastic, and on the back it says "You agree to the Contract contained inside this pack. Opening the pack denotes your agreement to the Contract". This would be explicitly a shrink- wrap contract, as you would be unable to read the contract before "agreeing" to it. However, you'd be unable to read the contract to determine whether you agreed or not.

You can see what's wrong, can't you? It's not fair, because morally you should be allowed to read the contract and then decide whether you want to sign it or not.

That's an explicit shrink- wrap contract, where its status of "shrink-wrap" is obvious. More insidious are implicit shrink- wrap contracts, where you have already spent your money and you are then forced to sign a contract in order to avoid the money being wasted. You are allowed to read the contract, but you have not much choice about signing it as you are in effect "under duress" to sign it, or "over a barrel".

Examples of explicit shrink- wrap contracts include some early "free Internet" CDs and other giveaway software which literally had shrink wrap and the contract inside, and something on the outside making a claim that if you opened the box then you agreed to the contract. Some software companies such as Microsoft have been called on the "shrink- wrap software" issue in the early times. Also see What to do if you don't agree to Microsoft Media Player 11. Once you've said "Yes", your machine is damaged and if you want to restore it, then unless you sign the contract, you have to do something clever to "roll back" the updates. It is, in principle, an explicit shrink- wrap contract. (Note that it doesn't need any thin plastic film to be shrink- wrap for the purposes of the definition).

Examples of implicit shrink- wrap contracts include the stuff to do with the Slingbox. The thing itself is good, but the way the contract has you over a barrel, is a problem. Also, OMG has a problem with their affiliate merchants being allowed to put implicit shrink- wrap contracts in place where the affiliate has to go to a lot of trouble before discovering there are "additional terms and conditions".

If you'd asked me a while ago if Adobe had a shrink- wrap contract for their Adobe Acrobat PDF Reader, I'd have said yes, it is a shrink- wrap contract. You had to download Adobe Acrobat in order to read the contract of software conditions which allowed or disallowed things to do with the software. However, this is no longer true because some people have written their own PDF readers, so you can break the deadlock by reading the Adobe contract without having to download the software first. Also see Clauses in Contracts and Legal Stuff

13.2 Needs on this contract

The legal status of shrink wrap contracts in the US is somewhat unclear. In the 1980s, software license enforcement acts were enacted by Louisiana and Illinois in an attempt to address this issue, but parts of the Louisiana act were invalidated in Vault Corp. v. Quaid Software Ltd., and the Illinois act was quickly repealed.[1] Case history also fails to clear up the confusion. One line of cases follows ProCD v. Zeidenberg which held such contracts enforceable (see, e.g., Bowers v. Baystate Technologies[2]) and the other follows Klocek v. Gateway, Inc., which found the contracts at hand unenforceable (e.g., Specht v. Netscape Communications Corp.[3]), but did not comment on shrink wrap contracts as a whole. These decisions are split on the question of consent, with the former holding that only objective manifestation of consent is required while the latter require at least the possibility of subjective consent. In particular, the Netscape contract was rejected because it lacked an express indication of consent (no "I agree" button) and because the contract was not presented directly to the user (users were required to click on a link to access the terms). However, the court in this case did make it clear that "Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility." Specht, 306 F.3d 17.

It may be worth noting that the user in the Zeidenberg case had purchased and opened the packages of multiple copies of the product, and therefore could not easily prove he remained ignorant of the contract/license; whereas in many cases, the so-called shrink-wrap "license" agreement has not been reviewed at the time of purchase (having been hidden inside the box), and therefore is arguably not part of the implicit legal agreement accompanying the sale of the copy, and is thus not enforceable by either party without further "manifestation of assent" to its terms. In general, a user is not legally obligated to read, let alone consent to any literature or envelope packaging that may be contained inside a product; otherwise such transactions would unduly burden users who have no notice of the terms and conditions of their possession of the object purchased, or the blind, or those unfamiliar with the language in which such terms are provided, etc. At the very least, the fair trade laws of most U.S. states would grant a buyer the right to cancel the purchase of a product where an enclosed contract provides terms of which purchaser cannot be aware at the time the product is purchased

13.3Indian Legislative Response to shrink wrap contract

Currently, the status of shrink wrap agreements is unclear. Courts have been split as to whether a consumer consents to the terms in a shrink wrap agreement since he pays for the product and goes so far as to open the package, but does not have actual knowledge of what the terms are until he opens the package to read them. - See more at: http://www.legalmatch.com/law-library/article/shrink-wrap-agreements.html#sthash.4OKikad0.dpuf

13.4 Relevant cases

ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), is a United States contract case involving a "shrink wrap license". One issue presented to the court was whether a shrink wrap license was valid and enforceable. Judge Easterbrook wrote the opinion for the court and found such a license was valid and enforceable. The Seventh Circuit's decision overturned a lower court decision.

Contents

1. Facts

The case involved a graduate student, Matthew Zeidenberg, who purchased a telephone directory database, SelectPhone, on CD-ROM produced by ProCD. ProCD had compiled the information from over 3,000 telephone directories, at a cost of more than $10 million. To recoup its costs, ProCD discriminated based on price by charging commercial users a higher price than it did to everyday, non-commercial users.

Zeidenberg purchased a non-commercial copy of SelectPhone and after opening the packaging and installing the software on his personal computer, Zeidenberg created a website and offered the information originally on the CD to visitors for a fee that was less than what ProCD charged its commercial customers.

At the time of purchase, Zeidenberg may not have been aware of any prohibited use; however, the package itself stated that there was a license enclosed. Moreover, because "the software license splashed across the screen and would not let him proceed without indicating acceptance," Zeidenberg had ample opportunity to read the license before using SelectPhone. Zeidenberg

was presented with this license when he installed the software, which he accepted by clicking assent at a suitable dialog box—this type of license is commonly known as a click-through license or clickwrap. The license was contained, in full, on the CD.

Vault Corp. v Quaid Software Ltd. 847 F.2d 255 (5th Cir. 1988) is a case heard by the United States Court of Appeals for the Fifth Circuit that tested the extent of software copyright. The court held that making RAM copies as an essential step in utilizing software was permissible under §117 of the Copyright Act even if they are used for a purpose that the copyright holder did not intend. It also applied the "substantial noninfringing uses" test from Sony Corp. of America v. Universal City Studios, Inc. to hold that Quaid's software, which defeated Vault's copy protection mechanism, did not make Quaid liable for contributory infringement. It held that Quaid's software was not a derivative work of Vault's software, despite having approximately 30 characters of source code in common. Finally, it held that the Louisiana Software License Enforcement Act clause permitting a copyright holder to prohibit software decompilation or disassembly was preempted by the Copyright Act, and was therefore unenforceable.

13.5 Misuse of technology in the form of shrink wrap contract

Internet technology has had such a profound effect on the rapid growth and development of electronic commerce that "e-commerce," a phrase used to describe a wide range of commercial transactions conducted on or through the Internet including everything from retail and direct marketing, to the purchase of software and information services, is now part of our everyday vocabulary.

As commerce on the Internet has grown, the inevitable fallout from failed transactions and business relationships has resulted in a developing body of case law. In some cases, the legal issues that govern the analysis of the electronic commercial transaction are no different from those applied in a more traditional commercial setting. For example, a fraudulent scheme perpetrated through print media is still the same fraudulent scheme when perpetrated on a web-site. Indeed, in the area of consumer fraud, the emerging issues in e-commerce are less related to substantive legal principles, than they are to procedural issues, such as the courts' jurisdiction over out-of-state defendants and discovering and stopping fraud from taking place online.

13.6 Summary

One contract issue that has received a good deal of attention by commentators, including the drafters of Article 2B, if not by the courts, and highlights the unique issues of contract formation and assent in transactions involving the Internet and the sale of "information," is the enforceability of "clickwrap" and "shrink- wrap" agreements.

13.7 References

James A.R. Nafziger & Ruan Jiafang. (1987). Chinese Methods of Resolving International Trade, Investment, and Maritime Disputes, 23 Willamette L.Rev. 619, 622, 676.

1) James R. Maxeiner. (2003). Standard-Terms Contracting in the Global Electronic Age: European Alternatives, 28 Yale J. Int'l L. 109, 118.
2) Jane C. Ginsburg. (1995). Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace, 95B Colum. L. Rev. 1466, 1472 n.23 (defining shrink- wrap license as contract of adhesion).
3) Jerry D. Monroe, ProCD. Inc. v. Zeidenberg: An Emerging Trend in shrink-wrap Licensing?, 1 MARQ. INTELL. PROP. L. REV. 143
4) Katheryn A. Andresen. (July 2000). UCITA and other US laws in an international perspective, *Journal of Internet Law,* volume 4, number 1.

13.8 Check your progress

1) _____ and _____ is posing a great deal of threat to the Society,
2) _____ of the Information Technology Act, 2000 penalizes cyber contract.
3) _____ is something that tends to excite lust.

13.9 Answers to check your progress

1) Shrink wrap
2) Contract matter
3) Transaction suspect
4) Lascivious

13.10 Terminal Questions

1. What is the difference between shrink wrap and click wrap
2. What do you mean by cyber agreement?
3. What all are the laws for shrink wrap contract described under IT Act, 2000?

Unit-14
Concept of convergence, Interest Telephony and CPNS

OBJECTIVES

After going through this unit you should be able to:

- Understanding the concept of convergence.
- Understanding the legal scenario of convergence according to cyber space.
- Understanding the flaws of current scenario.

Structure

14.1 Introduction

Telecommunications convergence, network convergence or simply convergence are broad terms used to describe emerging telecommunications technologies, and network architecture used to migrate multiple communications services into a single network.[1] Specifically this involves the converging of previously distinct media such as telephony and data communications into common interfaces on single devices, such as most smart phones can make phone calls and search the web.

The rise of digital communication in the late 20th century has made it possible for media organizations (or individuals) to deliver text, audio, and video material over the same wired, wireless, or fiber-optic connections. At the same time, it inspired some media organizations to explore multimedia delivery of information. This digital convergence of news media, in particular, was

called "Mediamorphosis" by researcher Roger Fidler [2], in his 1997 book by that name. Today, we are surrounded by a multi-level convergent media world where all modes of communication and information are continually reforming to adapt to the enduring demands of technologies, "changing the way we create, consume, learn and interact with each other".[2]

Convergence in this instance is defined as the interlinking of computing and other information technologies, media content, and communication networks that has arisen as the result of the evolution and popularization of the Internet as well as the activities, products and services that have emerged in the digital media space. Many experts[who?] view this as simply being the tip of the iceberg, as all facets of institutional activity and social life such as business, government, art, journalism, health, and education are increasingly being carried out in these digital media spaces across a growing network of information and communication technology devices.

Also included in this topic is the basis of computer networks, wherein many different operating systems are able to communicate via different protocols. This could be a prelude to artificial intelligence networks on the Internet eventually leading to a powerful superintelligence[3] via a technological singularity.

Convergent services, such as VoIP, IPTV, Mobile TV, Smart TV, and others, tend to replace the older technologies and thus can disrupt markets. IP-based convergence is inevitable and will result in new service and new demand in the market.[4]

When the old technology converges into the public-owned common, IP based services become access-independent or less dependent. The old service is access-dependent.

14.1.1 What is concept of convergence (Right Interest telephony and cpns)

1. Communication networks were designed to carry different types of information independently. Radio was designed for audio, and televisions were designed for video. The older media, such as television and radio, are broadcasting networks with passive audiences. Convergence of telecommunication technology permits the manipulation of all forms of information, voice, data, and video. Telecommunication has changed from a world of scarcity to one of seemingly limitless capacity. Consequently, the possibility of audience interactivity morphs the passive audience into an engaged audience.[15]
2. The historical roots of convergence can be traced back to the emergence of mobile telephony and the Internet, although the term properly applies only

from the point in marketing history when fixed and mobile telephony began to be offered by operators as joined products. Fixed and mobile operators were, for most of the 1990s, independent companies. Even when the same organization marketed both products, these were sold and serviced independently.

3. In the 1990s an implicit and often explicit assumption was that new media was going to replace the old media and Internet was going to replace broadcasting. In Nicholas Negroponte's *Being Digital*, Negroponte predicts the collapse of broadcast networks in favor of an era of narrow-casting. He also suggests that no government regulation can shatter the media conglomerate. "The monolithic empires of mass media are dissolving into an array of cottage industries.... Media barons of today will be grasping to hold onto their centralized empires tomorrow.... The combined forces of technology and human nature will ultimately take a stronger hand in plurality than any laws Congress can invent."[16] The new media companies claimed that the old media would be absorbed fully and completely into the orbit of the emerging technologies.
4. George Gilder dismisses such claims saying, "The computer industry is converging with the television industry in the same sense that the automobile converged with the horse, the TV converged with the nickelodeon, the word-processing program converged with the typewriter, the CAD program converged with the drafting board, and digital desktop publishing converged with the Linotype machine and the letterpress." Gilder believes that computers had come not to transform mass culture but to destroy it.
5. Media companies put Media Convergence back to their agenda, after the dot-com bubble burst. Erstwhile Knight Ridder promulgated concept of portable magazines, newspaper, and books in 1994.

14.3 Legal Scenario

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.

14.4 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.

Misuse of Internet telephony 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.

14.6 Summary

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.

14.7 References

- Good practice guide for computer-based electronic evidence (.pdf) by ACPO (English Wales & N Ireland). Retrieved from: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
- Managing containers, content and context in digital preservation: towards a 2020 vision (.pdf) by Simon Tanner; King's College London (UK). Retrieved from: http://www.kdcs.kcl.ac.uk/fileadmin/documents/pubs/Simon_Tanner_IST_2006paper.pdf
- Accountability for archival digital curation in preserving the memory of the world (.pdf) by Wayne W. Liu, Dept. of Computer Science, Florida State University. Retrieved from:

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/VC_Liu_26_D_1540.pdf

- Defining Digital Forensic examination and analysis tools using abstraction layers (.pdf) by Brian Carrier, Research Scientist (International Journal of Digital Evidence, Winter 2003, Vol.1, Issue 4) Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf
- British Library Digital Preservation Strategy (.pdf) Retrieved from: http://www.bl.uk/aboutus/stratpolprog/collectioncare/discovermore/digitalpreservation/strategy/DigitalPreservationStrategy2007-08.pdf
- Electronic Evidence And Computer Forensics (.pdf) by Linda Volonino, Information Systems and Telecommunications, Canisius College (Communications of the Association for Information Systems, vol. 12, Article 27, Oct. 2003). Retrieved from: http://faculty.usfsp.edu/gkearns/Articles_Fraud/Fraud_Deterrence.pdf
- Searching and Seizing Computers and obtaining electronic evidence in criminal investigations (.pdf) by H. Marshall Jarrett (Director, EOUSA) and Michael W. Bailie (Director, OLE), OLE Litigation Series, Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys. Retrieved from: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
- Digital Evidence: Representation and Assurance (.pdf) by Bradley Schatz, Bachelor of Science, UQ, Australia, 1995, published by Queensland University of Technology, Oct. 2007. Retrieved from: http://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf
- Issues in Computer Forensics (.pdf) by Sonia Bui, Michelle Enyeart, Jenghuei Luong, COEN 150, Dr. Holliday, May 22, 2003. Retrieved from: http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf
- Computer Forensics- We've had an incident, who do we get to investigate? (.pdf) by Karen Ryder, GSEC Certification Assignment Version 1.3, published at SANS. Retrieved from: https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652
- Anti-Cartel Enforcement Manual (.pdf), Published in International Competition Network (March 2010). Retrieved from:

http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf

- International Standard, ISO/IEC 27037 (.pdf), First Edition 2012-10-15
- Chapter-5 & 6, Pg. No. 121-161, Computer Forensics: Computer Crime Scene Investigation by John R. Vacca (ISBN 1-58450-018-2), Charles River Media, Inc., Hingham, Massachusetts.

14.8 Check your progress

1. Evidence should be _____.
2. The evidence which is presented in front of jury should be _____ and _____.
3. The major step followed for controlling the contamination of evidences is the _____.
4. _____ is a mandatory process in the field of investigation.
5. A _____ should be consulted in case of preserving business servers.

14.9 Answers to check your progress

1. Authentic
2. Understandable and believable
3. Chain of custody
4. Computer convergence
5. Computer specialist

14.10 Terminal Questions

1. Discuss the steps of preserving digital evidence.
2. Describe the methods of collecting digital evidence.
3. How digital evidence is processed in court of law?
4. What is the difference between computer convergence methods?

Unit-15

Legislative Framework to deal Cyber Space

OBJECTIVES

After going through this unit you should be able to:

- Understanding the protection of human rights in cyberspace.
- Understanding the cyber security strategies that violate human rights.
- Understanding the law of privacy and statutory perspective.

Structure

15.1 Introduction

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.[74] 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.[75]

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

[74] Public Privacy Human Rights in Cyber Space by Anja Mihr; retrieved from http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf

[75] Public Privacy Human Rights in Cyber Space by Anja Mihr; retrieved from http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf

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.

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 venture) 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.

15.2 Protection in cyberspace[76]

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 “Privacy 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

[76] Digital Privacy: Protecting Human Rights in Cyberspace by Doug Bannerman; retrieved from http://www.symantec.com/connect/blogs/digital-privacy-protecting-human-rights-cyberspace

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."

15.3 Human Rights in Cyber Space[77]

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.

[77] Public Privacy Human Rights in Cyber Space by Anja Mihr; retrieved from http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf

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 Charta) 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.

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.

15.4 Adopting cyber security strategies that violate human rights[78]

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

[78] Cyber Security, Cyber Surveillance and Online Human Rights by Anja Kovacs et.al.; retrieved from http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf

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.

15.5 Constitutional mandates[79]

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

[79] Data Protection Law in India: A Constitutional Perspective by Praveen Dalal; retrieved from http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-IN-INDIA.pdf

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.

15.6 Information Technology and the Law of Privacy[80]

Advances in computer technology and telecommunications have dramatically increased the amount of information that can be stored, retrieved, accessed and collected almost 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 impossible not long ago. Information in many databases can be cross-matched to create profiles of individuals and to even predict their behaviour. This behaviour 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:

i. 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

[80] Data Protection Law in India: A Constitutional Perspective by Praveen Dalal; retrieved from http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-IN-INDIA.pdf

where you shopped and when, what you bought, your brand preferences, your favorite restaurant.

ii. 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 opinion 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 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.

15.7 Statutory perspective[81]

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.

[81] Data Protection Law in India: A Constitutional Perspective by Praveen Dalal; retrieved from http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-IN-INDIA.pdf

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.

15.8 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.

15.9 Summary

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.

15.10 References

1. Public Privacy Human Rights in Cyber Space by Anja Mihr; retrieved from http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf
2. Digital Privacy: Protecting Human Rights in Cyberspace by Doug Bannerman; retrieved from http://www.symantec.com/connect/blogs/digital-privacy-protecting-human-rights-cyberspace
3. Cyber Security, Cyber Surveillance and Online Human Rights by Anja Kovacs et.al.; retrieved from http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
4. Data Protection Law in India: A Constitutional Perspective by Praveen Dalal; retrieved from http://ipmall.info/hosted_resources/gin/PDalal_DATA-PROTECTION-LAW-IN-INDIA.pdf

15.11 Check your progress

1. Electronic Communications Privacy Act of 1986 is the act of _____.
2. Article 19(1) (a), are available only to citizens of _____.
3. Freedom of speech and expression is discussed under _____.
4. _____ enshrines right to life and personal liberty.
5. _____ which aims to allow individuals have access to internet at any time.

15.12 Answers to check your progress

1. U.S.
2. India
3. Article 19 (1) (a)
4. Article 21
5. Right to Internet

15.13 Terminal Questions

1. How would you protect your privacy in virtual world?
2. Discuss, how cyber security strategies violates human rights?
3. Explain some constitutional mandates which relates to privacy and human rights?
4. Explain the difference between privacy and human rights?
5. How IT Act, 2000 involve itself in the law of privacy?

Unit-16
Open Source Movement

OBJECTIVES

After going through this unit you should be able to:

- Understanding the OSM and nature of Open source movement.
- Understanding the OSM with its drawbacks and future perspective.

StructureIntroduction

16.1 Introduction

The open source movement is a broad-reaching movement of individuals who support the use of open source licences for some or all software.[*citation needed*]. Open source software is made available for anybody to use or modify, as its source code is made available. Some open-source software is based on a share-alike principle, whereby users are free to pass on the software subject to the stipulation that any enhancements or changes are just as freely available to the public, while other open-source projects may be freely incorporated into any derivative work, open-source or proprietary.[1] Open source software promotes learning and understanding through the dissemination of understanding.[*citation needed*] The main difference between open-source and traditional proprietary software is in user and property rights, the conditions of use imposed on the user by the software license, as opposed to differences in the programming code.[*citation needed*] With open source software, such as OpenOffice.org, users are

granted the right to both the program's functionality and methodology.[2] With proprietary software programs, such as Microsoft Office, users only have the rights to functionality.[3] Examples of popular open source software products include Mozilla Firefox, Google Chromium, Android and OpenOffice.org.

Programmers who support the open source movement philosophy contribute to the open source community by voluntarily writing and exchanging programming code for software development.[4] The term “open source” requires that no one can discriminate against a group in not sharing the edited code or hinder others from editing their already-edited work. This approach to software development allows anyone to obtain and modify open source code. These modifications are distributed back to the developers within the open source community of people who are working with the software. In this way, the identities of all individuals participating in code modification are disclosed and the transformation of the code is documented over time.[5] This method makes it difficult to establish ownership of a particular bit of code but is in keeping with the open source movement philosophy. These goals promote the production of “high quality programs” as well as “working cooperatively with other similarly minded people” to improve open source technologies.[4]

In the late 1970s and early 1980s, two different groups were establishing the roots of the current open source software movement. On the United States eastern coast, Richard Stallman, formerly of the MIT AI lab, created the GNU project and the Free Software Foundation.[6] The GNU project was aimed to create a free operating system, and used the GNU General Public License (GPL) as the software license to prohibit proprietization of the software, but allow redistribution and modification.

On the U.S. West coast, the Computer Science Research Group (CSRG) of the University of California at Berkeley was adding improvements to the original Unix operating system from AT&T, and developed many applications, which became known as "BSD Unix". These efforts were funded mainly by DARPA contracts[*citation needed*], and a dense network of Unix hackers around the world helped to debug, maintain and improve the system.[7] During 1991–1992, two significant events took place:

In 1993, both GNU/Linux and 386BSD were reasonably stable platforms. Since then, 386BSD has evolved into a family of BSD-based operating systems (NetBSD, FreeBSD, and OpenBSD), while the Linux kernel is used in many GNU/Linux distributions such as Slackware, Debian, Red Hat, SUSE, Mandrake, and many more.[7]

The label “open source” was created and adopted by a group of people in the free software movement at a strategy session[8] held at Palo Alto, California, in reaction to Netscape's January 1998 announcement of a source code release for Navigator. One of the reasoning behind using the term was that "the [advantage] of using the term open source [is] that the business world usually tries to keep free technologies from being installed." [9] Those people who adopted the term used the opportunity before the release of Navigator's source code to free themselves of the ideological and confrontational connotations of the term "free software". Later in February 1998, Bruce Perens and Eric S. Raymond founded an organization called Open Source Initiative (OSI) “as an educational, advocacy, and stewardship organization at a cusp moment in the history of that culture.” [10]

16.2 Evolution of OSM

1. In the beginning, a difference between hardware and software did not exist. The user and programmer of a computer were one and the same. When the first commercial electronic computer was introduced by IBM in 1952, the machine was hard to maintain and expensive. Putting the price of the machine aside, it was the software that caused the problem when owning one of these computers. Then in 1952, a collaboration of all the owners of the computer got together and created a set of tools. The collaboration of people were in a group called PACT (The Project for the Advancement of Coding techniques). After passing this hurdle, in 1956, the Eisenhower administration decided to put restrictions on the types of sales AT&T could make. This did not stop the inventors from developing new ideas of how to bring the computer to the mass population. The next step was making the computer more affordable which slowly developed through different companies. Then they had to develop software that would host multiple users. MIT computation center developed one of the first systems, CTSS (Compatible Time-Sharing System). This laid the foundation for many more systems, and what we now call the Open Source Movement.[11]
2. The Open Source Movement is branched from the free software movement which began in the late 80s with the launching of the GNU/Linux project by Richard Stallman.[5] Stallman is regarded within the open source community as sharing a key role in the conceptualization of freely shared source code for software development.[5] The term “free software” in the free software movement is meant to imply freedom of software exchange and modification. The term does not refer to any monetary freedom.[5] Both the free software

movement and the open source movement share this view of free exchange of programming code, and this is often why both of the movements are sometimes referenced in literature as part of the FOSS or "Free and Open Software" or FLOSS "Free/Libre Open Source" communities.

3. These movements share fundamental differences in the view on open software. The main, factionalizing difference between the groups is the relationship between open source and proprietary software. Often makers of proprietary software, such as Microsoft, may make efforts to support open source software to remain competitive.[12] Members of the open source community are willing to coexist with the makers of proprietary software[5] and feel that the issue of whether software is open source is a matter of practicality.[5]
4. In contrast, members of the free software community maintain the vision that all software is a part of freedom of speech[5] and that proprietary software is unethical and unjust.[5] The free software movement openly champions this belief through talks that denounce proprietary software. As a whole the community refuses to support proprietary software. It also is suggested there are external motivations exist for these developers. One motivation is when a programmer fixes a bug or makes a program it benefits others in an open source environment. Another motivation is that a programmer can work on multiple projects that they find interesting and enjoyable. Programming in the open source world can also lead to commercial job offers or entrance into the venture capital community. These are just a few reasons why open source programmers continue to create and advance software.[13]
5. While cognizant of the fact that both it and the open source movement share similarities in practical recommendations regarding open source, the free software movement fervently continues to distinguish themselves from the open source movement entirely.[5] The free software movement maintains that it has fundamentally different attitudes towards the relationship between open source and proprietary software. The free software community does not view the open source community as their target grievance, however. Their target grievance is proprietary software itself.[5]

16.5 Misuse of OSM

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 OSM proceeding electronically.

16.6 Legal Aspects

1. The Open Source Movement has faced a number of legal challenges. Companies that manage open source products have some difficulty securing their trademarks. For example, the scope of “implied license” conjecture remains unclear and can compromise an enterprise’s ability to patent productions made with open source software. Another example is the case of companies offering add-ons for purchase; licensees who make additions to the open-source code that are similar to those for purchase may have immunity from patent suits.
2. In the court case "Jacobsen v. Katzer", the plaintiff sued the defendant for failing to put the required attribution notices in his modified version of the software, thereby violating license. The defendant claimed Artistic License in not adhering to the conditions of the software’s use, but the wording of the attribution notice decided that this was not the case. "Jacobsen v Katzer" established open source software’s equality to proprietary software in the eyes of the law.
3. In a court case accusing Microsoft of being a monopoly, Linux and open source software was introduced in court to prove that Microsoft had valid competitors and was grouped in with Apple.
4. There are resources available for those involved open source projects in need of legal advice. The Software Freedom Law Center features a primer on open source legal issues. International Free and Open Source Software Law Review offers peer-reviewed information for lawyers on free software issues.

16.7 Formalization

1 Richard Stallman, a supporter of the free software movement, was one of the free software movement advocates who proposed an alternative to the private models prevalent in the industry. After developing a non proprietary operating system called GNU, Stallman founded the Free Software Foundation in 1983. For most of the 1970s and 1980s, organizations such as AT&T, with their Unix operating system initiative, have promoted a policy of shared source code.

2 Linus Torvalds then built upon Stallman’s development in the late 1980s and created the Linux operating system that he released under Stallman’s GNU

General Public License. This enabled open source programmers to improve, modify, and develop his system.[14]

3 The Open Source Initiative (OSI) was also instrumental in the formalization of the Open Source Movement. The OSI was founded by Eric Raymond and Bruce Perens in February 1998 with the purpose of providing general education and advocacy of the open source label through the creation of the Open Source Definition that was based on the Debian Free Software Guidelines. The OSI has become one of the main supporters and advocators of the open source movement.[15]

4 In February 1998 the open source movement was adopted, formalized, and spearheaded by the Open Source Initiative (OSI), an organization formed to market software "as something more amenable to commercial business use"[5] The OSI owns the trademark "Open Source"[4] The main tool they adopted for this was the Open Source Definition[16]

5 The "open source" label was conceived at a strategy session that was held on February 3, 1998 in Palo Alto, California and on April 8 of the same year, the attendees of Tim O'Reilly's Free Software Summit voted to promote the use of the term "open source".[15]

6 Overall, the software developments that have come out of the open source movement have not been unique to the computer science field, but they have been successful in developing alternatives to propriety software. Members of the open source community improve upon code and write programs that can rival much of the propriety software that is already available.[5]

7 The rhetorical discourse used in open source movements is now being broadened to include a larger group of non-expert users as well as advocacy organizations. Several organized groups such as the Creative Commons and global development agencies have also adopted the open source concepts according to their own aims and for their own purposes.[17]

8 The factors affecting the Open Source Movement's legal formalization are primarily based on recent political discussion over copyright, appropriation, and intellectual property.[18]

16.8 Summary

OSM 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. OSM 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.

16.9 References

1 Definition of Open Source : Open Source Initiative Retrieved 2012-08-03

2 Get Involved : Apache Foundation Retrieved on 2012-08-03.

3 Bradley, D.A. (2005). "The divergent anarcho-utopian discourses of the open source software movement". *Canadian Journal of Communication* 30: 585–611.

Wyllys, R.E. (2000). Overview of the Open-Source Movement. Retrieved November 22, 2009, from The University of Texas at Austin Graduate School of Library & Information Science

4 Warger, T. (2002). The Open Source Movement. Retrieved November 22, 2009, from Education Resources Information Center

5 Richard Stallman. The GNU Project. In Chris DiBona, Sam Ockman, and Mark Stone, editors, Open Sources. Voices from the Open Source Revolution. O'Reilly & Associates, 1999

6 A brief history of open source software. Eu.conecta.it. Retrieved on 2011-11-30.

7 Tiemann, Michael (September 19, 2006). "History of the OSI". Open Source Initiative. Retrieved August 23, 2008.

8 A Brief History of the Open-Source Movement. Sloanreview.mit.edu (2011-11-18). Retrieved on 2011-11-30.

9 History of the OSI | Open Source Initiative. Opensource.org. Retrieved on 2011-11-30.

10 Weber, Steven. The Success of Open Source. The President and Fellows of Harvard College. 2004. Print pg.20–28. This whole paragraph is referenced to Steven Weber

16.10 Check your progress

1. OSM debuted in _____ in United States.
2. OSM generally used for solving _____ disputes in online medium.
3. _____ and _____ Model of OSM

.

16.11 Answers to check your progress

1. 1998
2. Business

16.12 Terminal Questions

1. Describe the nature of OSM.
2. Discuss why OSM is important.
3. What are the drawbacks of OSM?
4. What all are the benefits of OSM?

Unit-17
Drafting of Cyber Contract: Practical Approach

OBJECTIVES

After going through this unit you should be able to:

- Understanding the phenomenon of law enforcement agencies.
- Understanding the importance of trust and security on cyberspace.
- Understanding the scope and development of cyber laws.

Structure

17.1 Introduction

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.[82]

17.2 Importance of trust and security on Cyberspace[83]

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 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 legislations 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

[82] Cyber Law & Information Technology by Talwant Singh, Addl. Distt. & Sessions Judge, Delhi; retrieved from http://delhidistrictcourts.nic.in/CYBER%20LAW.pdf

[83] Cyber-Laws and Enforcement by Ajmal Edappagath, Supreme Court, New Delhi (India), IIMAHD, Vol. 14, No. 3, December 2004; retrieved from http://www.iimahd.ernet.in/egov/ifip/dec2004/article2.htm

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.

17.3 Scope and Development of Cyber Laws[84]

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 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.

Table 1: Scope and Development of ICT Legislations

[84] Cyber-Laws and Enforcement by Ajmal Edappagath, Supreme Court, New Delhi (India), IIMAHD, Vol. 14, No. 3, December 2004; retrieved from http://www.iimahd.ernet.in/egov/ifip/dec2004/article2.htm

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	N.A.	N.A.	ITU & ISO standards

jurisdiction			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 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 corporate 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').

17.4 Future Aspects[85]

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.

[85] Cyber-Laws and Enforcement by Ajmal Edappagath, Supreme Court, New Delhi (India), IIMAHD, Vol. 14, No. 3, December 2004; retrieved from http://www.iimahd.ernet.in/egov/ifip/dec2004/article2.htm

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*".

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.

17.5 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.

17.6 Summary

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.

17.7 References

1) Cyber Law & Information Technology by Talwant Singh, Addl. Distt. & Sessions Judge, Delhi; retrieved from http://delhidi strictcourts.nic.in n/ CYBER%20LAW.pdf
2) Cyber-Laws and Enforcement by Ajmal Edappagath, Supreme Court, New Delhi (India), IIMAHD, Vol. 14, No. 3, December 2004; retrieved from http://www.iimahd.ernet.in/egov/ifip/dec2004/article2.htm

17.8 Check your progress

1. NISA stands as _____.
2. Name one European cybercrime agency _____.
3. When was ENISA established? In the year _____.
4. NCSC stands for _____.
5. World Summit on the Information Society (WSIS) led by _____.

17.9 Answers to check your progress

1. European and Network Information Security Agency
2. European and Network Information Security Agency
3. 2004
4. National Cyber Security Center

5. ITU

17.10 Terminal Questions

1. What are the various pragmatic approaches at national, regional and international levels for cybercrime?
2. How challenges of cross-border cyber-crimes are faced at regional and international levels?
3. Discuss any two international conventions on cybercrime.
4. What are the future aspects of enforcement agencies against cybercrime?
5. Discuss some areas where development of cyber laws are must.

Unit-18
New Challenges in Current Regime of Cyber Space

OBJECTIVES

After going through this unit you should be able to:

- Understanding the misuse of technology under Indian Penal Code, 1860.
- Understanding the offences and special laws covered under IPC.
- Understanding adjudication process of Information Technology Act, 2000.

Structure

18.1 Introduction

The Indian Penal Code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often

referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.[86]

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463,464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.[87]

18.2 Misuse of Information Technology under Indian Penal Code, 1860[88]

S.No.	Section	Offence Name	Description	Penalty
1.	Various sections		The IT Act amends the IPC. The word document now includes an electronic record. The result is that anyone using forged electronic record or certificates is punishable under the IPC for offences related to false evidences and certificates.	Imprisonments for terms which may extend to 10 years or with fine or with both.
2.	120 A	Criminal Conspiracy	Two or more persons agree to do an illegal act or an act by illegal means themselves or through some other persons or means.	Depending on the object of Conspiracy imprisonment for

[86] Cyber Laws in India retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

[87] India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective by Rohit K. Gupta; retrieved from http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

[88] Seth Associates (Advocates & Legal consultants); retrieved from http://www.sethassociates.com/criminal-liability-for-misuse-of-information-technology.html

				term from 6 months to life imprisonment with or without fine.
3.	153 A (1)	Promoting enmity between different groups	By words spoken or written, signs, visible representations or otherwise attempting to promote or promotion of enmity between different groups on grounds of religion, race, domicile, residence, language etc.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
4.	292	Sale, etc., of obscene books, etc.	Selling, hiring, distribution, public exhibition or putting into circulation of obscene material, taking part or receiving profits of such business, advertisement etc.	On first conviction imprisonment up to 2 years with fine of 2000 Rupees on second or sequent conviction imprisonment up to 5 years with fine of 5000 Rupees.
5.	295 A	Deliberate and malicious acts, intended to outrage religious feelings of any class	Using words, signs or visible representations with deliberate and malicious intention to outrage religious feelings of a religious class.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
6.	463	Forgery	Making any false electronic record or a part of it with the intention to cause damage or injury to public or any person to commit any fraud or enter into any express or implied contract.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
7.	416	Cheating by	Cheating by pretending to be	Imprisonment

		personating	some other person or by knowingly substituting one person for another person representing that he or any other person is a person other he or such other person really is. Person personated could be a real or imaginary person.	for a term which may extend to 2 years, or with fine or with both.
8.	499	Defamation	Whoever by words either spoken or intended to be read or by signs or by visible representations makes or publishes any imputation concerning any person intending to harm the reputation of such person is said to defame.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
9.	501	Printing or engraving matter known to be defamatory	Printing or engraving any matter knowing or having good reason to believe that such matter is defamatory.	Imprisonment for a term which may extend to 2 years, or with fine or with both.
10.	503	Criminal Intimidation	Threatening another with any injury to his person, reputation or property or to some person in whom one is interested with the intention to cause alarm to that person or causing him to do any illegal act in order to avoid the threat.	Imprisonments for a term which may extend from 2 years till 7 years, with fine or with both depending on the kind of threat given.
11.	505(1), (2)	Statements conducing to public mischief	Making, publishing or circulating any rumour or false report about armed forces of India or with intention to create enmity, hatred or ill-will between classes.	Imprisonment for a term which may extend to 3 years, or with fine or with both.
12.	507	Criminal Intimidation by	Criminal Intimidation by anonymous communication or	Imprisonments for a term which

		anonymous communication	having taken precaution to conceal name and whereabouts of the person giving threat.	may extend from 2 years till 7 years, with fine or with both depending on the kind of threat given and 2 years additional imprisonment.
13.	509	Word, gesture or act intended to insult the modesty of a woman	Utterance of words, making of sound, gesture or exhibition of object in order to intrude the privacy or insult the modesty of a woman.	Imprisonment for a term which may extend to 1 year, or with fine or with both.

18.3 Offences covered under IPC and Special Laws[89]

7.3.1 Sending threatening messages by email

Sec.503 IPC

Section 503 Criminal intimidation

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

Explanation-A threat to insure the reputation of any deceased person in whom the person threatened is interested, is within this section.

7.3.2 Sending defamatory messages by email

Sec. 499 IPC

Section 499 Defamation

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such

[89] Alert India.com, retrieved from http://www.alertindian.com/node/5

imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, of defame that person.

Explanation 1-It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2-It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3-An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4-No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

7.3.3 Forgery of electronic records, Email spoofing

Sec 463, 464, 468, 469 IPC

Section 463 Forgery

Whoever makes any false documents or electronic record part of a document or electronic record with, intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

Section 464: Making a false document

A person is said to make a false document or false electronic record-

First-Who dishonestly or fraudulently-

a) Makes, signs, seals or executes a document or part of a document;
b) Makes or transmits any electronic record or part of any electronic record;
c) Affixes any digital signature on any electronic record;
d) Makes any mark denoting the execution of a document or the authenticity of the digital signature,

With the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alterations.

Section 468 Forgery for purpose of cheating

Whoever commits forgery, intending that the 1[document or Electronic Record] forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 469 Forgery for purpose of harming reputation

Whoever commits forgery, 1[intending that the document or Electronic Record forged] shall harm the reputation of any party, or knowing that it is likely to use for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

7.3.4 Bogus websites, cyber frauds

Sec 420 IPC

Section 420 Cheating and dishonestly inducing delivery of property

Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

7.3.5 Web-Jacking

Sec. 383 IPC

Section 383 Extortion

Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits "extortion".

7.3.6 E-Mail Abuse, Online Defamation

Sec.500, 509 IPC

Section 500 Punishment for defamation

Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.

Section 509 Word, gesture or act intended to insult the modesty of a woman

Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, of that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

7.3.7 Criminal Intimidation by E-mail or Chat

Sec. 506, 507 IPC

Section 506 Punishment for criminal intimidation

Whoever commits, the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both;

If threat be to cause death or grievous hurt, etc.: -And if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or 1[imprisonment for life], or with imprisonment for a term which may extend to seven years, or to impute, unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

Section 507 Criminal intimidation by an anonymous communication

Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person form whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence by the last preceding section.

7.3.8 Online sale of Drugs

-NDPS Act

7.3.9 Online sale of Arms

-Arms Act

7.3.10 Piracy

-Sec. 51, 63, 63 B Copyright act

When copyright infringed:- Copyright in a work shall be deemed to be infringed ---

(a) when any person, without a license granted by the owner of the Copyright or the Registrar of Copyrights under this Act or in contravention of the conditions of a license so granted or of any condition imposed by a competent authority under this Act ---

(i) Does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or

(ii) Permits for profit any place to be used for the performance of the work in public where such performance constitutes an infringement of the copyright in the work unless he was not aware and had no reasonable ground for believing that such performance would be an infringement of copyright, or

(b) When any person ---

(i) Make for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or

(ii) Distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright, or

(iii) By way of trade exhibits in public, or

(iv) Imports (except for the private and domestic use of the importer) into India, any infringing copies of the work.

Explanation- For the purposes of this section, the reproduction of a literary, dramatic, musical or artistic work in the form of a cinematograph film shall be deemed to be an "infringing copy".

Section 63 Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of-

(a) The copyright in a work, or

(b) Any other right conferred by this Act, 125[except the right conferred by section 53A]shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees :

Provided that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgement, impose a sentence of imprisonment for a term of less than six months or a fine of less than fifty thousand rupees.

Explanation-Construction of a building or other structure which infringes or which, if completed, would infringe the copyright in some other work shall not be an offence under this section.

63A Enhanced penalty on second and subsequent convictions -

Whoever having already been convicted of an offence under section 63 is again convicted of any such offence shall be punishable for the second and for every subsequent offence, with imprisonment for a term which shall not be less than one year but which may extend to three years and with fine which shall not be less than one lakh rupees but which may extend to two lakh rupees: Provided that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgment impose a sentence of imprisonment for a term of less than one year or a fine of less than one lakh rupees: Provided further that for the purposes of this section, no cognizance shall be taken of any conviction made before the commencement of the Copyright (Amendment) Act, 1984.

63B Knowing use of infringing copy of computer programme to be an offence.

Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees:

Provided that where the computer programme has not been used for gain or in the course of trade or business, the court may, for adequate and special reasons to be mentioned in the judgment, not impose any sentence of imprisonment and may impose a fine which may extend to fifty thousand rupees."

7.3.11 Obscenity

Sec. 292,293,294 IPC, Indecent Representation of Women Act

Section 292 Sale, etc., or obscene books, etc.

(1) For the purposes of sub-section

(2) a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(3) Whoever-

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

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

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

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

(e) Offers or attempts to do any act which is an offence under this section, Shall be punished 4[on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees.

Exception-This section does not extend to-

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

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

(ii) Which is kept or used bona fide for religious purposes?

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

(i) Any ancient monument within the meaning or the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

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

Section 292A Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail

Whoever, -

(a) Prints or causes to be printed in any newspaper, periodical or circular, or exhibits or causes to be exhibited, to public view or distributes or causes to be distributed or in any manner puts into circulation any picture or any printed or written document which is grossly indecent, or in scurrilous or intended for blackmail, or

(b) Sells or lets for hire, or for purposes of sale or hire makes, produces or has in his possession, any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail; or

(c) Conveys any picture or any printed or written document which is grossly indecent or is scurrilous or intended for blackmail knowing or having reason to believe that such picture or document will be printed, sold, let for hire distributed or publicly exhibited or in any manner put into circulation; or

(d) Takes part in, or receives profits from, any business in the course of which he knows or has reason to believe that any such newspaper, periodical, circular, picture or other printed or written document is printed, exhibited, distributed, circulated, sold, let for hire, made, produced, kept, conveyed or purchased; or

(e) Advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any Act which is an offence under this section, or that any such newspaper, periodical, circular, picture or other printed or written document which is grossly indecent or is scurrilous or intended for blackmail, can be procured from or through any person; or

(f) Offers or attempts to do any act which is an offence under this section *[shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Provided that for a second or any subsequent offence under this section, he shall be punished with imprisonment of either description for a term which shall not be less than six months and not more than two years.

Explanation I-For the purposes of this section, the word scurrilous shall be deemed to include any matter which is likely to be injurious to morality or is calculated to injure any person:

Provided that it is not scurrilous to express in good faith anything whatever respecting the conduct of-

(i) A public servant in the discharge of his public functions or respecting his character, so far as his character appears in that conduct and no further; or

(ii) Any person touching any public question, and respecting his character, so far as his character appears in that conduct and no further.

Explanation II-In deciding whether any person has committed an offence under this section, the Court shall have regard inter alia, to the following considerations-

(a) The general character of the person charged, and where relevant the nature of his business;

(b) The general character and dominant effect of the matter alleged to be grossly indecent or scurrilous or intended for blackmail;

(c) Any evidence offered or called by or on behalf of the accused person as to his intention in committing any of the acts specified in this section.

Section 293 Sale, etc., of obscene objects to young person

Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished 2[on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees.

Section 294 Obscene acts and songs

Whoever, to the annoyance of others-

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

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

7.3.12 Theft of Computer Hardware

Sec. 378, 379 IPC

Section 378 Theft

Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Explanation1 -A thing so long as it is attached to the earth, not being movable property, is not the subject of theft; but it becomes capable of being the subject of theft as soon as it is severed from the earth.

Explanation 2 -A moving effected by the same act which affects the severance may be a theft.

Explanation3 -A person is said to cause a thing to move by removing an obstacle which prevented it from moving or by separating it from any other thing, as well as by actually moving it.

Explanation 4 -A person, who by any means causes an animal to move, is said to move that animal, and to move everything which, in consequence of the motion so caused, is moved by that animal.

Explanation 5 -The consent mentioned in the definition may be expressed or implied, and may be given either by the person in possession, or by any person having for the purpose authority either express or implied.

Section 379 Punishment for theft

Whoever commits theft shall be punished with imprisonment of either description fora term which may extend to three years, or with fine, or with both.

Sony.Sambandh.Com Case[90]

A complaint was filed by Sony India Private Ltd which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients.

In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The

[90] Cyber Crimes: Law and Practices (.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call center in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the color television and the cordless head phone. The court convicted Arif Azim for cheating under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

Parliament Attack Case[91]

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also crafty made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

[91] Cyber Crimes: Law and Practices (.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

18.4 Section 46 (Power to adjudicate – Adjudicating Officer)[92]

Empowers the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry regarding the commission of the offences laid out in Chapter IX in the manner prescribed by the Central Government. The persons appointed shall possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction. This is also discussed in S. Sekar v. The Principal General Manager (Telecom), (BSNL), MANU/TN/9663/2007.

Every adjudicating officer appointed as above shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Section 58(2). Further all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 and it shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973.

The adjudicating officer shall offer the offender a reasonable opportunity for making representation in the matter. If, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of the Act governing such offence.

18.5 What is a Cybercrime?[93]

Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cybercrime. The Indian Law has not given any definition to the term 'cybercrime'. In fact, the Indian Penal Code does not use the term 'cybercrime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication

[92] Seminar and Workshop on detection of cybercrime and investigation by Justice K.N. Basha; retrieved from http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf

[93] Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6

device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

18.6 What is Cyber Law?

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cybercrimes have been declared as penal offences punishable with imprisonment and fine.

18.7 Use of Internet and Computers by Terrorists[94]

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

The scenario

The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people. E.g. one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible.

Terrorists also use physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. They also use virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

The law

[94] Real world cybercrime cases by Rohas Nagpal, Asian School of Cyber Laws; retrieved from http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/real-world-cyber-crime-cases.pdf

Terrorists are covered by conventional laws such as Indian Penal Code and special legislation relating to terrorism.

Who is liable?

Terrorists as well as those who help them to protect their information are liable. If email service providers do not assist the law enforcement personnel in the investigation then they are also legally liable.

The motive

Keeping terrorism related information confidential. Secure communication amongst terrorist group members.

Modus Operandi

The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

18.8 Misuse of technology

Cases involving misuse of Internet / Emails is not maintained separately by Government. However, as per the general cybercrime data maintained by National Crime Records Bureau, a total of 217, 288, 420 and 966 Cyber Crime cases were registered under Information Technology Act during 2007, 2008, 2009, 2010 respectively, thereby showing an increasing trend. A total of 339, 176, 276 and 356 cybercrime cases were reported under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009, 2010 respectively.

18.9 Summary

In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well. The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents.

18.10 References

1. Cyber Laws in India retrieved from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

2. India: An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective by Rohit K. Gupta; retrieved from
a. http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective
3. Seth Associates (Advocates & Legal consultants); retrieved from http://www.sethassociates.com/criminal-liability-for-misuse-of-information-technology.html
4. Alert India.com, retrieved from http://www.alertindian.com/node/5
5. Cyber Crimes: Law and Practices (.pdf); retrieved from http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
6. Seminar and Workshop on detection of cybercrime and investigation by Justice K.N. Basha; retrieved from
a. http://www.hcmadras.tn.nic.in/jacademy/article/Cyber%20Crime%20by%20KNBJ.pdf
7. Types of Cyber Crimes & Cyber Law in India by Adv. Prashant Mali, Security Corner; retrieved from http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6
8. Real world cybercrime cases by Rohas Nagpal, Asian School of Cyber Laws; retrieved from http://dict.mizoram.gov.in/uploads/attachments/cyber_crime/real-world-cyber-crime-cases.pdf

18.11 Check your progress

1. Section 420 of IPC deals with _____and dishonestly inducing delivery of property
2. _____ is a term used to describe the legal issues related to use of communications technology.
3. _____ deals with power to adjudication under IT Act, 2000.
4. Section 464 of _____ refers in matter of making a false document.
5. Section 499 of Indian Penal Code deals with _____.

18.12 Answer to check your progress

1) Cheating
2) Cyber law
3) Section-46

4) Indian Penal Code

5) Defamation

18.13 Terminal Questions

1) Describe defamation as per discussed in Indian Penal Code.

2) Discuss in detail section 420 of Indian Penal Code.

3) Explain how terrorists use internet technology to commit crime?

4) Discuss power of adjudication.

5) Explain Sony sambandh case under Indian Penal Code?