UNIT-1
INTRODUCTION

Under Amendment Act 2009

(Digital Signature Replace With Word Electronic Signature And Its Certificate Also Under Amendment Act 2009)

1	**Concept and Definition – Computer, Digital Signature, Key Pair, Subscriber, Verification**
2	Globalization and Ecommerce – U.S./U.K.
3	I.T. Act 2000 – Aim and object, E-mail, Torts & contract on Internet, Offences and Cyber Crimes, Stalking, Hacking, tempering, Junk Spaming – publication of obscene material, offences of computer, worms & virus Defamation and internet
4	Loop holes in I.T. Act.

Historical Background

New communication systems and digital technology have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of the advantages which the electronic form of business provides, people are reluctant to conduct business or conclude and transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates need for paper based transactions. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance, are the requirements of writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate e-commerce, the need for legal changes has become an urgent necessity. The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999. In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand 'what are the various perspectives of the IT Act, 2000 and what it offers?' The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. This Act was amended by Information Technology Amendment Bill 2008, passed in Loksabha and in Rajyasbha on in 2009.

For **IT AA-2008**, which are given as follows:

- The new amendments to the Information Technology Act, 2000 that got passed by the Lok Sabha last December deserve a careful reading. There are a number of positive developments, as well as many which dismay. Positively, they signal an attempt by the government to create a dynamic policy that is technology neutral. This is exemplified by its embracing the idea of electronic signatures as opposed to digital signatures. But more could have been done on this front (for instance, section 76 of the Act still talks of floppy disks). There have also been attempts to deal proactively with the many new challenges that the Internet poses.
- The word Electronic signature and electronic certificate use in place of digital signature and certificate.
- **Freedom of Expression**
  The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (s.67B) has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Unfortunately, the section covers everyone who performs the conducts outlined in the section, including minors. A slight awkwardness is created by the age of "children" being defined in the explanation to section 67B as older than the age of sexual consent. So a person who is capable of having sex legally may not record such activity (even for private purposes) until he or she turns eighteen.
- Another problem is that the word "transmit" has only been defined for section 66E. The phrase "causes to be transmitted" is used in section 67, 67A, and 67B. That phrase, on the face of it, would include the recipient who initiates a transmission along with the person from whose server the data is sent. While in India, traditionally the person charged with obscenity is the person who produces and distributes the obscene material, and not the consumer of such material. This new amendment might prove to be a change in that position.
- Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Art. 19(1)(a) of our Constitution. The fact that some information is "grossly offensive" (s.66A(a)) or that it causes "annoyance" or "inconvenience" while being known to be false (s.66A(c)) cannot be a reasons 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 form 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 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests are specified, no guidelines have been specified. Those guidelines, per s.69A(2), "shall be such as may be prescribed". It has to be ensured that they

are prescribed first, before any powers of censorship are granted to anybody. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable (*In re Venugopa*l, AIR 1954 Mad 901).

- **Intermediary Liability**
  The amendment to the provision on intermediary liability (s.79) while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies.
- Firstly, the requirement of taking down content upon receiving "actual knowledge" is much too heavy a burden for intermediaries. Such a requirement forces the intermediary to make decisions rather than the appropriate authority (which often is the judiciary). The intermediary is no position to decide whether a Gauguin painting of Tahitian women is obscene or not, since that requires judicial application of mind. Secondly, that requirement is vitiates the principles of natural justice and freedom of expression because it allows a communication and news medium to be gagged without giving it, or the party communicating through it, any due hearing. It has been held by our courts that a restriction that does not provide the affected persons a right to be heard is procedurally unreasonable .
- The intermediary loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information. While the first two are required to be classified as true "intermediaries", the third requirement is a bit too widely worded. For instance, an intermediary might automatically inject advertisements in all transmissions, but that modification does not go to the heart of the transmission, or make it responsible for the transmission in any way. Similarly, the intermediary may have a code of conduct, and may regulate transmissions with regard to explicit language (which is easy to judge), but would not have the capability to make judgments regarding fair use of copyrighted materials. So that kind of "selection" should not render the intermediary liable, since misuse of copyright might well be against the intermediary's terms and conditions of use.
- **Privacy and Surveillance**
  While the threat of cyber-terrorism might be very real, blanket monitoring of traffic is not the way forward to get results, and is sure to prove counter-productive. It is much easy to find a needle in a small bale of hay rather than in a haystack. Thus, it must be ensured that until the procedures and safeguards mentioned in sub-sections 69(2) and 69B(2) are drafted before the powers granted by those sections are exercised. Small-scale and targetted monitoring of metadata (called "traffic data" in the Bill) is a much more suitable solution, that will actually lead to results, instead of getting information overload through unchannelled monitoring of large quantities of data. If such safeguards aren't in place, then the powers might be of suspect constitutionality because of lack of guided exercise of those powers.
- Very importantly, the government must also follow up on these powers by being transparent about the kinds of monitoring that it does to ensure that the civil and human rights guaranteed by our Constitution are upheld at all times.
- Encryption
  The amending bill does not really bring about much of a change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance), now the government may even call upon intermediaries to help it with decryption (s.69(3)). Additionally, s.118 of the Indian Penal Code has been amended to

recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offence punishable with death or imprisonment for life'.

- The government already controls the strength of permissible encryption by way of the Internet Service Provider licences, and now has explicitly been granted the power to do so by s.84A of the Act. However, the government may only prescribe the modes or methods of encryption "for secure use of the electronic medium and for promotion of e-governance and e-commerce". Thus, it is possible to read that as effectively rendering nugatory the government's efforts to restrict the strength of encryption to 40-bit keys (for symmetric encryption).
- **Other Penal Provisions**
  Section 66F(1)(B), defining "cyber terrorism" is much too wide, and includes unauthorized access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyber terrorism, it is tough to conceive of slander as a terrorist activity.
- Another overly broad provision is s.43, which talks of "diminish[ing] its value or utility" while referring information residing on a computer, is overly broad and is not guided by the statute. Diminishing of the value of information residing on a computer could be done by a number of different acts, even copying of unpublished data by a conscientious whistleblower might, for instance, fall under this clause. While the statutory interpretation principle of *noscitur a socii* (that the word must be understood by the company it keeps) might be sought to be applied, in this case that doesn't give much direction either.
- While all offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments (Airtel case, for instance), and frivolous cases that are being registered (Orkut obscenity cases).
- Cheating by personating is not defined, and it is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalized, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds (like Second Life) will be brought under the meaning of "personation" and "cheating".
- While it must be remembered that more law is not always an answer to dealing with problems, whether online or otherwise, it is good to note that the government has sought to address the newer problems that have arisen due to newer technologies. But equally important is the requirement to train both the judiciary and the law enforcement personnel to minimize the possibility of innocent citizens being harassed.

Information Technology Preamble

THE INFORMATION TECHNOLOGY ACT, 2000

Preamble

(No. 21 OF 2000)

[*9th June*, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows

Term:

- Preamble[1] (a basic frame work of an Act which show its object and scope)
- Electronic commerce[2]
- Modal law on electronic 1966 [3]
- UNICTRAL[4]

[1] A preliminary or preparatory statement; an introduction.

[2] the paperless exchange of business information using electronic data interchange (EDI), e-mail, electronic bulletin boards, fax transmissions, and electronic funds transfer

[3] http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf last access on 26feb 2015 refer for the Modal law

[4] http://www.uncitral.org/uncitral/ last access on 26feb 2015 for UNICTRAL detail

Modal Law

Purpose

The Model Law on Electronic Commerce (MLEC) purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade.

Why is it relevant?

The MLEC was the first legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence that are widely regarded as the founding elements of modern electronic commerce law. The principle of non-discrimination ensures that a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality mandates the adoption of provisions that are neutral with respect to technology used. In light of the rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. The functional equivalence principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfill the same purposes and functions that certain notions in the traditional paper-based system - for example, "writing," "original," "signed," and "record" - seek to achieve.

Key provisions

Besides formulating the legal notions of non-discrimination, technological neutrality and functional equivalence, the MLEC establishes rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages.

It should be noted that certain provisions of the MLEC were amended by the Electronic Communications Convention in light of recent electronic commerce practice. Moreover, part II of the MLEC, dealing with electronic commerce in connection with carriage of goods, has been complemented by other legislative texts, including the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (the "Rotterdam Rules") and may be the object of additional work of UNCITRAL in the future.

Important Definitions

Section 2	Definitions
Computer (I)	means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network
Digital Signature (P)	means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3; (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained u/s 3
Key Pair (X)	in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
Subscriber(Zg)	means a person in whose name the Digital Signature Certificate is issued.
Verification (Zh)	in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether— (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber; (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature
Access (A)	with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network
Asymmetric Crypto System (F)	means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature
Cyber Appellate Tribunal (N)	means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48
Data (O)	means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer
Intermediary(W)	with respect to any particular electronic message means any person who

	on behalf of another person receives, stores or transmits that message or provides any service with respect to that message
Originator(Za)	means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary[5];
Private Key (Zc)	means the key of a key pair used to create a digital signature
Public Key (Zd)	means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate
Communication Device (Ha)	means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)
Computer Security (Nb)	Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
Electronic Signature (Ta)	authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature
Electronic Signature Certificate (Tb)	an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate

Diff B/W Public &Private Key

Public Key vs. Private Key

Cryptography[6] is the study of hiding information, and it is used when communicating over an untrusted medium such as internet, where information needs to be protected from other third parties. Encryption uses an algorithm called a cipher to encrypt data and it can be decrypted only using a special key. Encrypted information is known as cipher text and the process of obtaining the original information (plaintext) from the cipher text is known as decryption. One of the two widely used encryption methods is Public Key Encryption (other being the Symmetric Key Encryption). Specialty of public key encryption is that two different but mathematically related keys called public key and private key are used (as opposed to symmetric key encryption, which uses the same private key for encryption and decryption).

Public key encryption encrypts data using the recipient's public key and it cannot be decrypted without using a matching private key. In other words, you need one key to lock (encrypt the pian text) and another key to unlock (decrypt the cyper text). Important thing is that one key cannot be used in the place of the other. Depending on which key is published, public key encryption can be used for two purposes.

What is Public Key?

In public key encryption, data encrypted using the recipient's public key cannot be decrypted without using a matching private key. On the other hand, the public key can be used to decrypt data encrypted by the matching private key. However, public key cannot be used in the place of the private key. If the locking key is made public, then this system can be used by anybody to send private communication

[5] mediator
[6] the art of writing or solving codes

to the holder of the unlocking key. This makes sure that the legal recipient (one who has the matching private key) is the only person able to read the message. So, this confirms confidentiality of the communication between two parties.

What is Private Key?

In public key encryption[7], the private key can only be used to decrypt the data that was encrypted using the matching public key. Similarly, data encrypted using private key can only be decrypted using the matching public key. However, the private key cannot be used in the place of the public key. If the locking key is made private, this system makes it possible to verify that the documents were locked by the owner. The reason is that a message encrypted by the sender can only be opened by a person with the matching public key, thus verifying that the sender did actually hold the private key (meaning that the original and non-tampered message has been received). Therefore, this is used for digital signatures.

What is the difference between Public Key and Private Key?

Public key and private key is the couple of keys used in public key cryptography. If the locking key is made public, then the unlocking key becomes the private key, and vice versa. Public key cannot be used to derive the private key. If the public key is the locking key, then it can be used to send private communication (i.e. to preserve confidentiality). If the private key is the locking key, then the system can be used to verify documents sent by the holder of the private key (i.e. to preserve authenticity).

IT Act 2000 has 13 chapter94 section and 4

Short detail via chart

1-14	**Digital signature legal aspects**
15-42	DSC
43-47	Penalties and compensation
48-64	Tribunal
65-79	Offences
80-94	Miscellaneous

Section wise detail

Sec 5	**DS[8] legal recognition**
Sec 15	Secure DS
Sec 43	Penalty for computer damages
Sec 61	Civil court
Sec 62	Appeal
Sec 63	Compounding
Sec 64	Recovery of penalty
Sec 65	Tampering
Sec 66	Hacking
Sec 67	Obscene
Sec 71	Penalty of misrepresentation
Sec 72	Privacy penalty

[7] Is the process of encoding messages or information in such a way that only authorized parties can read it.
[8] Digital signature

Sec 73	False DSC[9] penalty
Sec 74	Fraudulent publication
Sec 75	Conservation outside India
Sec 48	CAT[10]
Sec 51	CAT term
Sec 52	CAT salary qualification
Sec 56	CAT staff
Sec 60	Limitation

Some Leading Case Law

1. Pune Citibank MphasiS Call Center Fraud

- US $ 3, 50,000 from accounts of four US customers were dishonestly *transferred to bogus accounts*. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it are a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.
- The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers.
- All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.
- There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

2. Bazee.com case

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable *material was being sold on the website*. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

[9] Digital Signature Certificate
[10] Cyber appellant tribunal

3. State of Tamil Nadu Vs Suhas Katti

- The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

- The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.
- Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

- On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.
- The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.
- Further the Defense counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

- Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:
- " The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."
- The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

4. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. *The couple exchanged many emails using the company computers*. After some time the two broke up and the girl created *fraudulent email ids* such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

5 SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

- In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate reputation was being *defamed* through emails and passed an important ex-parte injunction.
- In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.
- On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant.
- After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.
- This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

4. PARLIAMENT ATTACK CASE

- 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 after computer experts at Delhi failed to trace much out of its contents.

- 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 craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

9. Andhra Pradesh Tax Case

- Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.
- The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.
- The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted.
- It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

8. SONY.SAMBANDH.COM CASE

- India saw its first cybercrime conviction recently. It all began after 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 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 under Section 418, 419 and 420 of the Indian Penal Code.
- The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre 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 colour television and the cordless head phone.In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim 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 the Indian Penal Code can be effectively applied to certain categories of cyber crimes 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.

9. Nasscom vs. Ajay Sood & Others

- In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `*phishing'* on the internet to be an illegal act, entailing an injunction and recovery of damages.
- Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a *bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc*. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.
- The Delhi HC stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image.
- The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.
- The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad-interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.
- The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.
- During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.
- This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

10. Infinity e-Search BPO Case

- The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed.
- A British newspaper had reported that one of its undercover reporters had *purchased personal information* of 1,000 British customers from an Indian call-center employee. However, the employee of Infinity eSearch , a New Delhi-based web designing company, who was reportedly involved in the case has denied any wrongdoing. The company has also said that it had nothing to do with the incident.
- In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.
- In this sort of a situation we can only say that the journalist has used "Bribery" to induce a "Out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter.

Section	Case	Held
66E	Jawaharlal Nehru University MMS scandal	In a severe shock to the prestigious and renowned institute - Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.
66F	Nagpur Congress leader's son MMS scandal	On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.
66F	Mumbai police	The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case.The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday.The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna," said an officer.
67	Yahoo	This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E - mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady's complaint, the police nabbed the accused. Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another

		person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet. Verdict: The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000. He is convicted and sentenced for the offence as follows: • As per 469 of IPC he has to undergo rigorous imprisonment for 2 years and to pay fine of Rs.500/- • As per 509 of IPC he is to undergo to undergo 1 year Simple imprisonment and to pay Rs 500/- • As per Section 67 of IT Act 2000, he has to undergo for 2 years and to pay fine of Rs.4000/-
67B	Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation:	The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.
69	Lakshmana Kailash K.,v Orkut	In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut. The police identified him based on IP address details obtained from Google and Airtel - Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m. Verdict: Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.
67	Avnish Bajaj v	Facts: There were three accused first is the Delhi school boy and IIT

State (N.C.T.) of Delhi (2005) 3 Comp LJ 364 (Del)	Kharagpur Ravi Raj and the service provider Avnish Bajaj. The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act 2000. In addition, the schoolboy faces a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines. Held: In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

IT capterization

Section 65 tempering with computer source documents

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

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

IT Aims, objective and short analysis

In May 2000, both the houses of the Indian Parliament passed the Information Technology[11] Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below:

- Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
- Act details about Electronic Governance and provides inter alia amongst others that 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 - rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Digital Signatures.
- Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates. Details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.
- Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.
- Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.
- Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking. The Act also provides for the constitution of the Cyber

[11] http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf refer if you want to read whole act.

Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Globalization & E-commerce US/UK/India

Electronic commerce, commonly known as E-commerce, is trading in products or services using computer networks, such as the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, marketing, online, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail.

E-commerce businesses may employ some or all of the following:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in prevail for launching new products and services

Work in E-commerce

Document automation in supply chain and logistic	Enterprise content management	Group buying
Print on demand	Automated online assistant	Newsgroups
Online shopping and order tracking	Online banking	Online office suites
Shopping cart software	Teleconferencing	Electronic tickets
Social networking	Instant messaging	Pretail

2. E-Commerce Governmental legislation

US

In the United States, some electronic commerce activities are regulated by the Federal Trade Commission (FTC). These activities include the use of commercial e-mails, online advertising and consumer privacy. The CAN-SPAM Act of 2003 establishes national standards for direct marketing

over e-mail. The Federal Trade Commission Act regulates all forms of advertising, including online advertising, and states that advertising must be truthful and non-deceptive. Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the FTC has brought a number of cases to enforce the promises in corporate privacy statements, including promises about the security of consumers' personal information. As result, any corporate privacy policy related to e-commerce activity may be subject to enforcement by the FTC.
The Ryan Haight Online Pharmacy Consumer Protection Act of 2008, which came into law in 2008, amends the Controlled Substances Act to address online pharmacies.
There is also collaboration between Google and US federal authorities to block illegal online pharmacies from appearing in Google search results. Recently FedEx Corporation pleaded not guilty to charges made against it regarding dealing with illegal online pharmacies.

UK
In the United Kingdom, The Financial Services Authority (FSA) was formerly the regulating authority for most aspects of the EU's Payment Services Directive (PSD), until its replacement in 2013 by the Prudential Regulation Authority and the Financial Conduct Authority. The UK implemented the PSD through the Payment Services Regulations 2009 (PSRs), which came into effect on 1 November 2009. The PSR affects firms providing payment services and their customers. These firms include banks, non-bank credit card issuers and non-bank merchant acquirers, e-money issuers, etc. The PSRs created a new class of regulated firms known as payment institutions (PIs), who are subject to prudential requirements. Article 87 of the PSD requires the European Commission to report on the implementation and impact of the PSD by 1 November 2012.

INDIA
In India, the Information Technology Act 2000 governs the basic applicability of e-commerce. It is based upon UNCITRAL Model but is not a comprehensive legislation to deal with e-commerce related activities in India. Further, e-commerce laws and regulations in India are also supplemented by different laws of India as applicable to the field of e-commerce. For instance, e-commerce relating to pharmaceuticals, healthcare, traveling, etc. are governed by different laws though the information technology act, 2000 prescribes some common requirements for all these fields. The competition commission of India (CCI) regulates anti competition and anti trade practices in e-commerce fields in India. Some stakeholders have decided to approach courts and CCI against e-commerce websites to file complaint about unfair trade practices and predatory pricing by such e-commerce websites.

Cyber Crime classification

Cyber crimes are classified into various types on the following basis:

1. Based on Old or New Crimes Committed on Computers Whether an old crime is committed on or through computer or a new crime is committed, cyber crimes are of following 3 types:

Crimes 'on' the Internet	Crimes 'of' the Internet	New crimes used for commission of old crimes
These are the old crimes which are committed on or through the new medium of the	These are new crimes created with the internet itself, such as hacking,	For e.g. where hacking is committed to carry out cyber fraud.

internet. For e.g. cheating, fraud, misappropriation, defamation, threats etc. committed on or through or with the help of the internet. The internet with its speed and global access has made these crimes much easier, efficient, risk-free, cheap and profitable to commit	planting viruses and IPR thefts.

Depending upon the victim of cyber crime, it may be broadly classified under the **Following 3 heads:**

Against Individuals Under this category it can be against individuals or against individual property through the means of:	**Against organizations, cyber crimes can be through the means of**	**Against society at large**
Harassment via e-mail	Unauthorized control/access over computer system	Pornography
Cyber stalking	Possession of unauthorized information	Indecent exposure
Dissemination of obscene material	Cyber terrorism against government organization	Trafficking
Defamation	Distribution of pirated software etc.	Financial crimes
Unauthorized control/access over computer system		Sale of illegal articles
Indecent exposure		Online gambling
E-mail spoofing		Forgery
Cheating and fraud		
Computer vandalism		
Transmitting virus		
Net trespass		
Intellectual property crimes		
Internet time thefts		

Based on Nature of Cyber Crime

Social cyber crime **Economic cyber crimes**

Social Cyber Crime	**Economic Cyber Crime**
Trafficking	Credit card schemes
Cyber terrorism	System corruption
Cyber fraud	Internet fraud
Cyber gambling	Dot com job scams

Cyber obscenity	Corporate and political espionage[12]
Pornography	Mafia and drug peddlers
	Multi site gambling websites

Cyber crime Characteristic

Low risk high rewarding ventures	**Lack of awareness among victims**	**Physical presence not required**
Lack of hi-tech skills among investigating agencies	Victims refrain from reporting cases	No violence is involved
No territorial boundaries	Anonymity and Openness	Paucity of authentic evidence
Have wider ramifications		
Phishing is a financial crime		

Cyber Hacking

i. Meaning of Hacking

Crime in the computer generated superhighway is the new phenomenon in contemporary scenario. In our daily life we cannot think of any intellectual and necessary work without Information Technology. But this new multimedia technology is being misused and abused by deviants and criminals. Hacking[13] attack on Bhaba Atomic Energy Centre, AIIMS, World Trade Centre etc. are examples of cyber hacking causing more harm to human life than traditional crimes. Therefore, to secure our daily life, business and every intellectual conduct we have to think of prevention and control of cyber crimes and specially of most dangerous one that is cyber hacking. The Information Technology Act 2000 does not define "cyber crimes". We may define cyber crimes as prohibited human conduct in computer generated superhighway or related to computer generated activities as well as related to other electronic devices which are Information Technology friendly, e.g., mobile phone, wireless, TV with internet connection etc. in the era of communication convergence. Those conducts are prohibited by State through Chapter-XI of the Information Technology Act, 2000 which is widely amended in the year 2009 and other related laws for example the Copyright Act, 1999 in India. *Sections 43 and 66 of the Information Technology Act, 2000 deal with hacking and other cyber crimes and prescribe punishments.* The Computer Misuse Act, 1990 in the United Kingdom and the Computer Fraud and Abuse Act, 1986 in the United States of America prescribe punishments for unauthorized access; the European Convention, 2000 recognized cyber hacking as cyber crime and so forth Hacking in cyberspace is not only national but also international legal challenge which requires global standard security measures and controlling policy through worldwide intensive study and research.

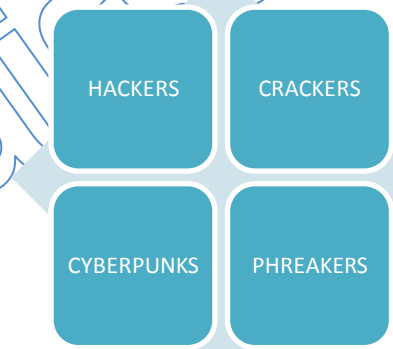
Hackers usually represent themselves as –

1. the protector of vulnerable and insecure information; and
2. their activities are within legal boundaries; and
3. that they are not always law-breakers.

[12] Spying

[13] gain unauthorized access to data in a system or computer.

Loop hole in that this may be because they are confident that –
a. Very few or only a few victims are interested to lodge complaint against them.
b. Most of the times victims are unable to identify them. This is due to unspecified and undefined jurisdiction in cyber world. The accused generally commit crime thousands and thousands of miles away.
c. Again another advantage for hackers for which they repeat crime commission is that it is very much complex to understand crime in cyberspace. For example, hackers view one webpage and by deep linking get information which are very confidential without the consent of owner and download it intentionally and dishonestly; it is a complete case of theft u/s 378 of the Indian Penal Code, 1860 that if any person with dishonest intention takes away any movable property from one place to another place without the consent of owner or possessor it is theft.
d. It is also very difficult to identify and understand the unauthorized use which is criminal trespass u/s 441 of the Indian Penal Code, 1860 as well as hackers who cause damage, after data or change data etc. Therefore, expert hackers think that cyberspace is their exclusive zone and they can do anything whatever they wish very tactfully. They not only cause harm to technological and economic dominion but also to the social, cultural and political values. *The term Hacker is used to describe any one of the following:*



a. HACKERS. They knew computers in and out. They can make the computer do nearly = everything they want it to do.
c. CRACKERS. They break into computer systems and security thereof.
d. CYBERPUNKS. They are the masters of cryptography.
e. PHREAKERS. They combine their in depth knowledge of the Internet and the mass

Hacker cases

Arrest of Computer Trainers at Chattisgarh: One Manoj Singhania, head of the local branch of Aptech and another Prakash Yadav, in-charge of training institute were arrested for allegedly sending e-mails in the name of Microsoft and Videsh Sancher Nigam Ltd. (VSNL) India. Those e-mails were containing programme file named 'Speed.exe.' At the moment file was opened it would automatically sent to accused the password, data and other information of the user. They had also tried to hack into the computers of the State Bank of India (SBI) in the same way.
Mr. Bhardwaj Case: In 2001, Mr. Bharadwaj, Managing Director of IGSP Technology Centre India Pvt. Ltd. filed an FIR at Chandigarh about hacking of 'computer system u/s 66 (1) and 66 (2) of the IT Act, 2000 and u/s 380 of the IPC, 1860 that Techno Noble Info Way Ltd. (TNIL) had illegally downloaded some data from their server in the U.S. The Police officers started immediate search of TNIL office premises and confiscated the server, related devices used in the crime. Though, accused's plea on the other hand was that IGSP committed breach of contract by not providing them minimum service as was agreed.

Judicial Response in India after the Information Technology Act, 2000

In Jayesh S. Thakkar v. State of Maharashtra,221 the petitioners wrote a letter to the Chief Justice of the Bombay High Court, about pornographic websites on the internet. The letter was treated as suo motu writ petition. The Bombay High Court passed an order to appoint a committee to suggest and recommend ways of preventive and controlling measure and means to protect children from access to pornographic and **obscene** material on the internet. A letter containing 'Terror Hits London' was left in internet with the help of a deadly Trojan virus and an online CNN news letter containing exclusive video footage on the terrorist attack after 7th July 2005 incidents of London blasts.313 It invites recipients to see the attachment and video shots. At the moment users started downloading, it started coping users system, accessed mail servers and others and started sending spam. More than 53,000 computers were infected by this Bo-box worms which contained Bin Laden or Saddam Hussein pictures.

Use of Trojan horse and viruses by terrorists It was breaking news in India on 16th July, 2005 that a Trojan virus posted as an online CNN news letter containing exclusive video footage of the terrorist attack with the words 'TERROR HITS LONDON' and invites recipients to see video shot attachments. The moment recipients started downloading the programme it started copying the users system and access the e-mail servers to send spam and junk mails. The spam mail contains the story of either death of Osama Bin Laden or Saddam Hussein and other data. More than 53,000 computers were affected.

Computer as a Victim of Crime

A computer or a computer network could be the target of an offence wherein the computer becomes the victim. In such cases, the computer's confidentiality, integrity, or accessibility is attacked. The information stored or the service provided by the victim is stolen or the victim is crippled and damaged. Such crimes involve disrupting the functioning of the computer, computer system or computer network; corrupt the operating systems and programmes; theft or disturb data or information; intellectual property violations and blackmail using personal information hacked from computer systems. Example of this form of computer crime is the denial of service attacks on popular internet sites like Yahoo, CNN etc. and the spread of the 'Melissa' and 'I Love You' viruses an d their variants.

Cyber Stalking

Historical Background of Stalking

Stalking is quite well-known as a phenomenon surrounding celebrities. But studies show that more than 80% of victims are 'ordinary' people. The fact that celebrities have been stalked, and even killed by their stalkers has helped in a way……it has brought the public eye on this phenomenon. The motivations of the stalker, the effect on the stalked and the manner in which the law ought to react have all been subjects of very detailed study in the aftermath of these celebrity-stalking. Many states in the US have enacted anti-stalking legislation after these incidents as well.

Meaning of Stalking

In very general terms, stalking refers to harassing or threatening behavior that an individual engages in repeatedly towards another person. Put slightly more crudely, it is a pattern of goal-directed behavior, both lawful and unlawful, promoted by a delusional and narcissistic perception of a relationship and intended to empower the 'predator' to feel omnipotent and in control, while reducing the 'prey's' emotional stability to a state of vulnerability and fear.In quasi-legal terms, stalking can be defined as a 'willful course of conduct' involving 'repeated or continuing harassment

of another individual' that 'actually causes' the victim to feel terrorized, frightened, intimidated, threatened, harassed or molested and that would cause a 'reasonable person' to feel so.

Meaning of Cyber Stalking

The 'Web' is no more and no less than a mirror of the real world and that means it also contains electronic versions of real life problems. Stalking is a problem that many people especially women, are familiar with in real life. These problems can occur on the internet as well, what has become known as 'Cyber Stalking' or 'on-line harassment'. It does not end here….there have been many examples of cyber stalking crossing over to real life stalking where even physical danger is of high probability.

Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through. However, as the Morris worm and Mydoom showed, even these "payload free" worms can cause major disruption by increasing network traffic and other unintended effects. A "payload" is code in the worm designed to do more than spread the worm—it might delete files on a host system (e.g., the ExploreZip worm), encrypt files in a extortion attack, or send documents via e-mail. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" computer under control of the worm author. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk email or to cloak their website's address. Spammers are therefore thought to be a source of funding for the creation of such worms, and the worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks.

Backdoors can be exploited by other malware, including worms. Examples include Doomjuice, which can spread using the backdoor opened by Mydoom, and at least one instance of malware taking advantage of the rootk it and backdoor installed by the Sony/BMG DRM software utilized by millions of music CDs prior to late 2005.

Junk spam[14]

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk

[14] Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited

mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

Virus

A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. 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 the user's 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, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. 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 life and evolutionary algorithms.

Computer viruses currently cause billions of dollars worth of economic damage each year, 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, due to its overwhelming popularity. Unfortunately, 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

Obscene material and IT law

WHAT IS OBSCENE

DEFINING OBSCENITY

The test for obscenity was first laid down the Regina v. Hicklin[15] as a "tendency to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall". Lord CJ Cockburn in his opinion in the Hicklin case explained that the danger of prurient literature was that it "would suggest to the minds of the young of either sex, and even to persons of more advanced years, thoughts of a most impure and libidinous character". In India, the Supreme Court in the case of Ranjit D. Udeshi v. State of Maharashtra[16] observed that the test laid down by Cockburn, C.J. should not be discarded. It observed:

> "that the test of obscenity to adopt in India is that obscenity without a preponderating social purpose or profit cannot have the constitutional protection of free speech and expression and obscenity in treating sex in a manner appealing to the carnal side of human nature or having that tendency. The obscene matter in a book must be considered by itself and separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book

[15] (1868) 3 QB 360.

[16] AIR 1965 SC 881.

> is likely to fall. In this connection the interests of our contemporary society and particularly the influence of the book on it must not be overlooked".

It further interpreted the word "obscene" as that which is "offensive to modesty or decency, lewd, filthy and repulsive". Also that section 292 of the IPC was a reasonable restriction on the right of freedom of speech and expression under Article 19 (2) of the Constitution.

In another case Samresh Bose v. Amal Mitra[17], the court held that:

> "the concept of obscenity would differ from country to country depending on the standards of morals of contemporary society". And that "obscenity has a tendency to deprave and corrupt those whose minds are open to such immoral influences".

Another test for obscenity is the Miller Test which was laid down by the United States Supreme Court in the case of Miller v. California.[18] It is a three-prong test for obscenity:

1. Whether the "average person", applying community standards would find the work, taken as a whole, appeals to the prurient interest;
2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically denied by state law;
3. Whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.

OBSCENITY IN ELECTRONIC FORM

In India, the Information Technology Act regulates obscene material in electronic form. Section 67 of the Act reads thus:

> "whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees".

The ingredients of an offence under this section are:

a) Publication or transmission in the electronic form.
b) Lascivious material appealing to prurient interests.
c) Tendency to deprave and corrupt persons.
d) Likely-audience
e) To read, see or hear the matter contained or embodied electronic form.

The word "publish" has not been defined under the Act. However, the Supreme Court held in the case of Bennett Coleman & Co. v. Union of India[19] that publish means "dissemination and circulation". In an electronic form, publication or transmission of information includes dissemination, storage and circulation. Information is defined under section 2 (1) (v) as "information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche. So, the obscene material could be in any of these forms to attract the offence of section 67. This section advocates that the 'obscene material in electronic form' must be considered by itself and separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the 'obscene material in the electronic form' is likely to fall.

---

17 AIR 1970 SC 1390.
18 413 US 15 (1973).
19 (1972) 2 SCC 788.

It is necessary to note that any offence related to obscenity in electronic form cannot be tried under section 292 of the IPC, as section 81 of the ITA states that the Act will have an overriding effect:

> "The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force."

Therefore, as a thumb rule, offences related to 'obscenity in electronic form' should be tried under the provisions of section 67 only and any attempt to import provisions of section 292 of IPC would tantamount to disregard of legislative intent behind the Act and cause miscarriage of justice.[20] But, in the recent judgment of Avnish Bajaj v. State (NCT of Delhi)[21] both the provisions were considered together in arriving at the judgment. Also, the punishment under section 67 of the ITA is more stringent that section 292 of the IPC. Section 67 is also criticized it is very easy for a person to escape criminal charges just by proving his lack of knowledge of publication or transmission of obscene information in the electronic form. Moreover, though publication or transmission of obscene information may be illegal but mere possession, browsing or surfing through obscene content is not an illegal activity.[22]

Case law

1. Maqbool Fida Husain v. Raj Kumar Pandey Delhi HC Crl. Rev. Pet. No. 280 and 282/2007. Judgement dated 08/05/2008.
2. Dr. Prakash v. State of Tamil Nadu (2002) 7 SCC 759.
3. Avnish Bajaj v. State (NCT of Delhi) decided on 29/05/2008, Delhi High Court Cri. M.C. 3066/2006.

IPC provision for Obscene and Defamation

292.A. 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,

---

[20] Vakul Sharma, Information Technology - Law and Practice, Universal Law Publishing, 2007, pg. 157.

[21] Avnish Bajaj v. State (NCT of Delhi) Delhi HC judgment dated 29/05/2008.

[22] Supra note 14 at pg. 156.

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.

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 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.

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, ballad 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.

CLASSIFICATION OF OFFENCE
Punishment—Imprisonment for 3 months, or fine, or both—Cognizable—Bailable—Triable by any Magistrate—Non-compoundable.

Section 499 of IPC
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 imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to 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.

First Exception —Imputation of truth which public good requires to be made or published.—It is not defamation to impute anything which is true concerning any person, if it be for the public good that the imputation should be made or published. Whether or not it is for the public good is a question of fact.

Second Exception—Public conduct of public servants.—It is not defamation to express in a good faith any opinion whatever respecting the conduct of a public servant in the discharge of his public functions, or respecting his character, so far as his character appears in that conduct, and no further.

Third Exception — Conduct of any person touching any public question.—It is not defamation to express in good faith any opinion whatever respecting the conduct of any person touching any public question, and respecting his character, so far as his character appears in that conduct, and no further.

Fourth Exception — **Publication of reports of proceedings of Courts.—**It is not defamation to publish substantially true report of the proceedings of a Court of Justice, or of the result of any such proceedings.

Explanation —A Justice of the Peace or other officer holding an inquiry in open Court preliminary to a trial in a Court of Justice, is a Court within the meaning of the above section.

Fifth Exception.—**Merits of case decided in Court or conduct of witnesses and others concerned.—**It is not defamation to express in good faith any opinion whatever respecting the merits of any case, civil or criminal, which has been decided by a Court of Justice, or respecting the conduct of any person as a party, witness or agent, in any such case, or respecting the character of such person, as far as his character appears in that conduct, and no further.

Sixth Exception—**Merits of public performance.—**It is not defamation to express in good faith any opinion respecting the merits of any performance which its author has submitted to the judgment of the public, or respecting the character of the author so far as his character appears in such performance, and no further.

Explanation —A performance may be substituted to the judgment of the public expressly or by acts on the part of the author which imply such submission to the judgment of the public.

Seventh Exception —Censure passed in good faith by person having lawful authority over another —It is not defamation in a person having over another any authority, either conferred by law or arising out of a lawful contract made with that other, to pass in good faith any censure on the conduct of that other in matters to which such lawful authority relates.

Eight Exception —Accusation preferred in good faith to authorized person.—It is not defamation to prefer in good faith an accusation against any person to any of those who have lawful authority over that person with respect to the subject-matter of accusation.

Ninth Exception—**Imputation made in good faith by person for protection of his or other's interests.—**It is not defamation to make an impu

Cyber Crime In India

Cyber crime In India

MODE AND MANNER OF COMMITTING CYBER CRIME:

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 no where 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 computerised.

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* wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

6. *Denial of Service attack-*

The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. *Amazon, Yahoo*.

7. *Virus / worm attacks-*

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. *love bug virus*, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by *Robert Morris* sometime in 1988. Almost brought development of Internet to a complete halt.

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 authorised 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 cyber criminal 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 cyber crime in India. However this case made the police infamous as to their lack of understanding of the nature of cyber crime.

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 as ransom. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

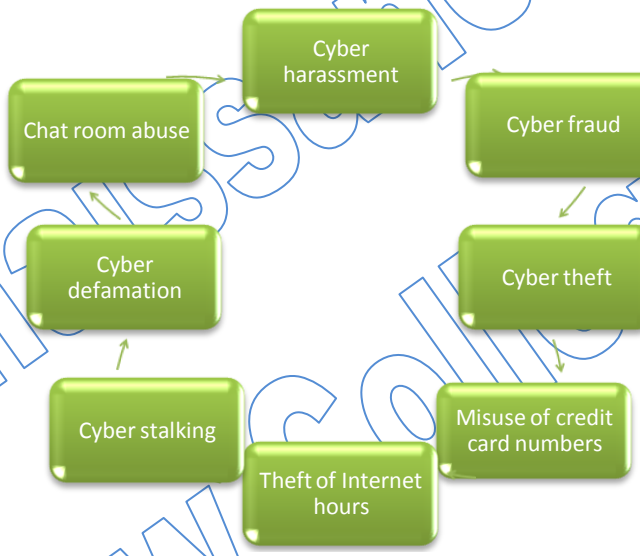
Loop Hole in IT

Besides the advantages that IT has, it also comes with many disadvantages. Though information technology has made communication easier and more convenient, it also left a bad site of it. . From cell phone signal interceptions to email hacking, people are now worried about their once private information becoming public knowledge. While information technology may have made the world a global village, it has also contributed to one culture dominating another weaker one. For example it is now argued that US influences how most young teenagers all over the world now act, dress and behave.

Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or 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 or for investigation of any offence. They can also secure assistance from computer personnel in decrypting data (see mandatory decryption), under penalty of imprisonment.

Section 66A is widely criticized. It has led to numerous abuses reported by the press. Section 66A has also been criticized and challenged in Lucknow and Madras High Courts for its constitutional validity. Based on Section 66A, Bombay High Court has held that creating a website and storing false information on it can entail cyber crime

1. The Information Technology Act, 2000 is likely to cause a conflict of jurisdiction.
2. Electronic commerce is based on the system of domain names. The Information Technology Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.
3. The Information Technology Act, 2000 does not deal with any issues concerning theprotection of Intellectual Property Rights in the context of the online environment.
4. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.
5. As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the Information Technology Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the Information Technology Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The Information Technology Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. These include:-



6. The Information Technology Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.
7. Another grey area of the Information Technology Act is that the same does not touch upon any anti- trust issues.
8. The most serious concern about the Indian Cyber law relates to its implementation. The Information Technology Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian cyber law raises more questions than it answers. It seems that the Parliament would be required to amend the Information Technology Act, 2000 to remove the grey areas mentioned above.
9. The Information Technology Act, 2000 does not touch at all the issues relating to Domain Names. Even Domain Names have not been defined and the rights and liabilities of Domain Name owners do not find any mention in the said law. It may be submitted that Electronic Commerce is based on the system of Domain Names and excluding such important issues from the ambit of India's First Cyber law does not appeal to logic.
10. Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

11. Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime.
12. Cyber torts- The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T.Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T.Act 2000 read with the Penal Code is capable of dealing with these felonies.
13. Cyber crime in the Act is neither comprehensive nor exhaustive- If that is the issue then the present legislation along with the Penal Code when read harmoniously and co- jointly is sufficient to deal with the present problems of cyber crime. Further there are other legislations to deal with the intellectual property crimes on the cyber space such as the Patents Act, Copy Right Act, and Trade Marks Act.
14. Ambiguity in the definitions- The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The infamous go2nextjob has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the citizen are till s. 66 exists in its present form. Further section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by the Bal Bharati case.
15. Uniform law- worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.
16. Lack of awareness- One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling Microsoft pirated software over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for online cheating by buying Sony products using a stolen credit card.
17. Jurisdiction issues- Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 is very silent on these issues.
18. Extra territorial application-Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies
19. Raising a cyber army- By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) **is** definitely a welcome step in this direction. There are man cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –

***Case 1*:** When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com. **Status:** Probe on

***Case 2*:** CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.
Status: Chargesheet not filed
Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

Status: Pak not cooperating.
21.Cyber savvy bench- Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. Mr T.K.Vishwanathan, member secretary, Law Commission, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated "if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System".
22. Dynamic form of cyber crime-Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind." The (de)creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.
23.Hesitation to report offences- As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the Delhi time theft case. "The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business."This attitude of the administration is also revelled by incident that took place at Merrut and Belgam. (for the facts of these incidents refer to naavi.com). For complete realisation of the provisions of this Act a cooperative police force is require.

Prevention of Cyber Crime

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security.

Precaution	*Prevention*	*Preservation*	*Protection*	*Perseverance*

A citizen should keep in mind the following things-
1.to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2.always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3.always use latest and update antivirus software to guard against virus attacks.

4.always keep back up volumes so that one may not suffer data loss in case of virus contamination
5.never send your credit card number to any site that is not secured, to guard against frauds.
6.always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7.it is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8.web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9.use of firewalls may be beneficial web servers running public sites must be physically separate protected from internal corporate network.

UNIT-2

ADJUDICATION AND PENALTIES

1	**Powers of Police Officers**
2	The Cyber Regulations Appellate Tribunal
3	Appeal to High Court
4	Compounding of contravention and Recovery of penalty

The Offence included in the ITAct 2000 are as follows

Tampering with the computer source documents.	**Hacking with computer system.**	**Publishing of information which is obscene in electronic form.**	**Power of Controller to give directions**
Directions of Controller to a subscriber to extend facilities to decrypt information	Protected system	Penalty for misrepresentation	Penalty for breach of confidentiality and privacy
Penalty for publishing Digital Signature Certificate false in certain particulars	Publication for fraudulent purpose	Act to apply for offence or contravention committed outside India	Confiscation
Penalties or confiscation not to interfere with other punishments.	Power to investigate offences.		

Power of Police Officer

78. Power to investigate offences.
Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of **Inspector** shall investigate any offence under this Act.
80. Power of police officer and other officers to enter, search, etc.
(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably

suspected or having committed or of committing or of being about to commit any offence under this Act

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.
(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Penalties, Compensation and Adjudication

43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means **(Inserted vide ITAA-2008)**
(i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

The shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

(i) "Computer Contaminant" means any set of computer instructions that are designed
  (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
  (b) by any means to usurp the normal operation of the computer, computer

system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

43 A Compensation for failure to protect data (Inserted vide ITAA 2006)

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008)

Explanation: For the purposes of this section

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

44 Penalty for failure to furnish information, return, etc

If any person who is required under this Act or any rules or regulations made thereunder to-

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations, fails to file return or furnish the same within the

time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45 Residuary Penalty

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

46 Power to Adjudicate

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), 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 in the manner prescribed by the Central Government. **(amended vide ITAA 2008)**

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore
Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five core shall vest with the competent court. (**Inserted Vide ITAA 2008**)

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.

(4) 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.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and –

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

(c) shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908 (Inserted vide ITAA 2008)

47 Factors to be taken into account by the adjudicating officer

While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely -

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;
(c) the repetitive nature of the default

Cyber Appellate Tribunal

48 Establishment of Cyber Appellate Tribunal

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49 Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008)

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint **(Inserted vide ITAA-2008)**

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008)

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. **(Inserted vide ITAA-2008)**

(3) Subject to the provisions of this Act-

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.**(Inserted vide ITAA-2008)**

(4) Notwithstanding anything contained in sub -section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench **(Inserted vide ITAA-2008)**

(5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. **(Inserted vide ITAA-2008)**

50 Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal (Substituted vide ITAA 2006)

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (substituted vide ITAA-2008)

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, and management or consumer affairs.

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years.

(Inserted vide ITAA-2008)
(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that service for a period of not less than five years.

51 Term of office, conditions of service etc of Chairperson and Members (Substituted vide ITAA 2008)
(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier. (Inserted vide ITAA 2008)
(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member. (Inserted vide ITAA 2008)
(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. (Inserted vide ITAA 2008)

52 Salary. allowance and other terms and conditions of service of Chairperson and Member. (Substituted vide ITAA 2008)
The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed: (Inserted vide ITAA 2008)

52A Powers of superintendence, direction, etc (Inserted vide ITAA 2008)
The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52B Distribution of Business among Benches (Inserted vide ITAA 2008)
Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench

52C Powers of the Chairperson to transfer cases (Inserted vide ITAA 2008)
On the application of any of the parties and after notice to the parties, and after hearing such

of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench

52D Decision by majority (Inserted vide ITAA 2008)

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

53 Filling up of vacancies (Amended vide ITAA 2008)

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding officer Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54 Resignation and removal (Amended vide ITAA 2008)

(1) The Presiding officer Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding officer Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding officer Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Presiding officer Chairperson or Member.

55 Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Inserted vide ITAA 2008)

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56 Staff of the Cyber Appellate Tribunal (Error in amendment...item 28)

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employes as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57 Appeal to Cyber Regulations Appellate Tribunal

(1) Save as provided in sub -section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of thesaid period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58 Procedure and Powers of the Cyber Appellate Tribunal

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

(a) summoning and enforcing the attendance of any person and examining him on oath;
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex parte
(g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed .to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59 Right to legal representation

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal Limitation

60 Limitation

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the

Cyber Appellate Tribunal.

61 Civil court not to have jurisdiction (Amended vide ITAA 2008)

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter. (Inserted vide ITAA 2006)

APPEAL TO HIGH COURT

62 Appeal to High court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within **sixty days** from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding **sixty days**.

63 Compounding of Contravention

(1) Any contravention under this Act [substituted for "Chapter" vide amendment dated 19/09/2002] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64 Recovery of Penalty or compensation (Amended vide ITAA 2006)

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall

be suspended till the penalty is paid.

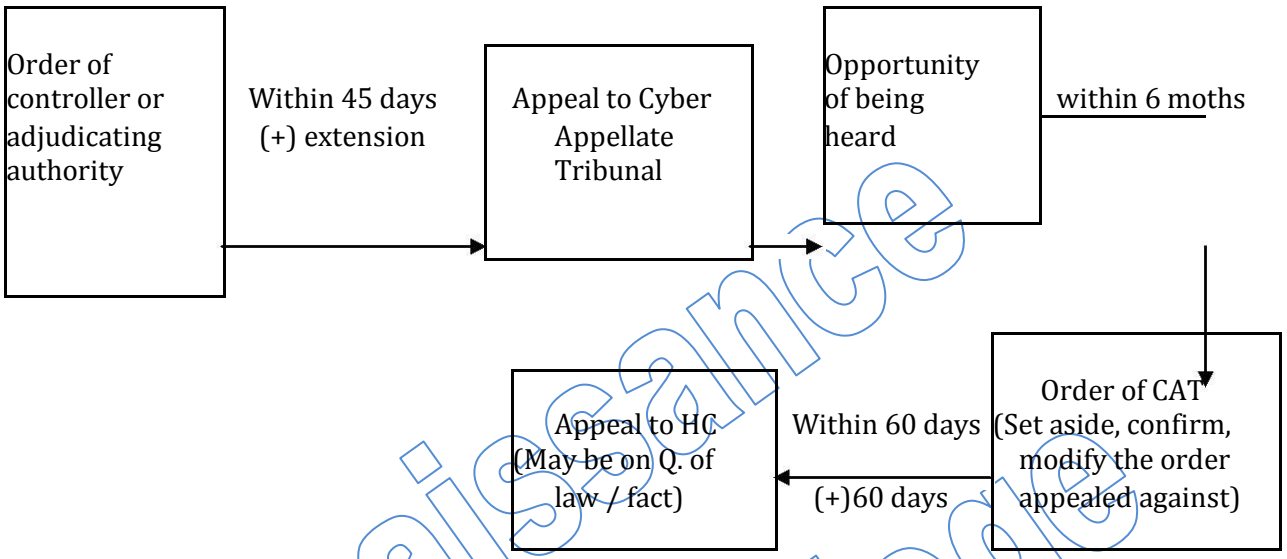
Offences and Punishment Chart

Sr. No.	Section	Offence	Punishment
1	65	Tampering with computer source documents	Imprisonment upto 3 years or fine upto Rs 2 lakh or both
2.	66	Computer related offences	Imprisonment upto 3 years or fine upto Rs 5 lakh or both
3.	66A	Sending offensive messages through communication device	Imprisonment upto 3 years and fine
4.	66B	Dishonestly receiving the stolen computer resource and communication device	Imprisonment upto 3 years or fine upto Rs. 1 lakh
5.	66C	Theft of identity	Imprisonment upto 3 years and fine upto Rs. 1 lakh
6.	66D	Cheating by personation by using computer resource or communication device	Imprisonment upto 3 years and fine upto Rs. 1 lakh
7.	66E	Violation of privacy	Imprisonment upto 3 years or fine upto Rs. 2 lakh or both
8.	66F	Cyber terrorism	Life imprisonment
9.	67	Publishing or transmitting obscene material in e-form	Upon 1st conviction with imprisonment upto 3 years and fine upto Rs 5 lakh; and upon 2nd or subsequent conviction with imprisonment upto 5 years and fine upto Rs 10 lakh
10.	67A	Publishing or transmitting material containing sexually explicit act in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
11.	67B	Publishing or transmitting material depicting children in sexually explicit act etc. in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.

12.	67C	Violating the directions to preserve and retain the information by intermediaries	Imprisonment upto 3 years and fine
13.	68	Violating the directions of Controller by Certifying Authority or his employee	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
14.	69	Violating the directions of the Central Government or State Government to a subscriber to extend facilities to decrypt information	Imprisonment upto 7 years and fine
15.	69A	Violating the directions to block any information for access by the public	Imprisonment upto 7 years and fine
16.	69B	Violating the directions to monitor and collect traffic data or information	Imprisonment upto 3 years and fine
17.	70 & 70A	Unauthorized access to a computer system	Imprisonment upto 10 years and fine
18.	70B	Violating the directions of the Indian Computer Emergency Response Team (CERT-IN)	Imprisonment upto 1 years or fine upto Rs 1 lakh or both
19.	71	Penalty for misrepresentation	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
20.	72	Penalty for breach of confidentiality and privacy	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
21.	72A	Disclosure of information in breach of lawful contract	Imprisonment upto 3 years or fine upto Rs 5 lakh or both
22.	73	Penalty for publishing electronic signature certificate false in certain particulars	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
23.	74	Publication for fraudulent purpose	Imprisonment upto 2 years or fine upto Rs 1 lakh or both

Penalties

Breach of confidentiality



Compounding of offences

- Either before or after institution of adjudication Compounded by Controller or Adjudicating Officer
- Similar contravention cannot be compounded within 3 yrs.

Power of CG to make rules (Sec 87)

By notification in the official gazette and in the electronic gazette Matters to be specified in the rules:

- Manner of authentication by means of digital signature
- Electronic form of filing, issue, payment etc.

Type and manner of affixing digital signature.

- Qualification, disqualification and terms & conditions of service of controller etc. Standards to be observed by controller
- Form and manner of application for license.
- Form for application for issue of digital certificate. etc.

Steps to create Digital Signature

- Electronic record is converted into "Message Digest" using mathematical function known as "Hash[23] Function" which freezes the electronic record.

[23] Confusion

- Private Key attaches itself to the message digest.

Liabilities of Companies

- Every person who was in-charge / responsible for day-to-day activity & the company shall be deemed to be guilty of such offense & shall be liable to be punished & proceeded against.
- Every Manager, Director, Officer with whose connivance such offense was committed shall also be liable.
- No liability if he proves his innocence.
- Controller shall act as repository for all digital signatures issued under this act.

Section	Case	Concept in sort

UNIT-3
PROTECTION OF CONSUMER AND VICTIMS

1	**Protection of consumer & unfair Terms**
2	Protection of person when person is not consumer
3	Proposed Amendments
4	R. B.I. Guideline for A.T.M. Transactions

Protection of Consumer and Unfair Victims

Consumer rights are an integral part of our lives like the consumerist way of life. We have all made use of them at some point in our daily lives. Market resources and influences are growing by the day and so is the awareness of one's consumer rights. These rights are well defined and there are agencies like the Government, consumer courts and voluntary organizations that work towards safeguarding. While we like to know about our rights and make full use of them, consumer responsibility is an area which is still not demarcated and it is hard to spell out that all the responsibility is that a consumer is supposed to shoulder.

Consumer Protection Act, 1986 is an important Act in the history of the consumer movement in the country. The Act was made to provide for the better protection and promotion of consumer rights through the establishment of consumer councils and quasi-judicial machinery. It is mile stone in the history of socio-economic legislation and directed towards public welfare and public benefits.

Consumer by an act

(d) **"Consumer"** means any person who, -

(i)Buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised or under any system of deferred payment when such use is made with the approval of such person but does not include a person who obtains such goods for resale or for any commercial purpose.(ii)[24][Hires or avails of] any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other then the person who [hires or avails of] the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person [but does not include a person who avails of such services for any commercial purpose];[25][Explanation. For the purposes of this sub-clause "commercial purpose" does not include use by a consumer of goods bought and used by him and services availed by him exclusively for the purposes of earning his livelihood, by means of self-employment;]

[24] Subs. By Act 50 of 1993, sec.2, for "hires" (w.r.e.f. 18-6-1993).
[25] Added by Act 62 of 2002, sec.2, (w.e.f. 15-3-1993).

(e) **"Consumer dispute"** means a dispute where the person against whom a complaint has been made, denies or disputes the allegations contained in the complaint;

Unfair term and Restrictive trade practice

The reliefs are:

-To discontinue them or not to repeat them (f);

Unfair trade practice and restrictive trade practice are defined in the Act with great precision. These words should be used only in cases contemplated in the definitions of those words, not in case of other grounds of complaint like defect in goods or overt-pricing, because the reliefs in such case are different. Some contract terms and conditions are individually agreed between you and the trader while others are standard terms that the trader uses for all customers. For example, you may individually agree the price with a trader but other terms, such as the right to cancel the contract, may be used in all the trader's contracts. Many written contracts contain standard terms, often in the small print. However, a standard term doesn't have to be in writing. For example, if a trader tells everyone that goods can be exchanged for any reason within 28 days this is a standard term.

What are unfair contract terms

Some contracts contain standard terms that the law says are unfair because they give the trader an unfair advantage over you, or take away your legal rights. The law which says these terms are unfair is called the **Unfair Terms in Consumer Contracts Regulations 1999.**

A term setting the price of the goods or services isn't unfair just because the price is high. However, a term allowing the trader to increase the price after you have made the agreement might be unfair.

Here are some examples of contract terms that may be unfair:

- any term which is very difficult to understand, perhaps because of the language or print size
- a term which tries to prevent you from carrying out your legal rights, for example, your right to a refund for faulty goods
- a term which tries to prevent you from taking a trader to court
- a term saying the trader is not responsible for a death or injury caused by something they have or haven't done
- a term saying the trader is not responsible for delays, even delays which are their fault
- a term saying the trader is not responsible if they don't do what they should do under the contract
- a term which tries to prevent you from keeping back payments when you have a genuine complaint about goods or services
- a term which tries to make you pay more than is needed to cover the trader's losses if you cancel the contract
- any term hidden from you until after you sign the contract
- a term giving the trader wide cancellation rights but not giving you the same rights
- a term giving the trader the right to change the contract to their benefit
- a term that makes it very difficult for you to end a contract - for example, a term making you pay high termination charges or give a long notice period.
- A term can't be unfair if you individually negotiated it with the trader and can't be unfair if the contract is between you and another private individual instead of a trader.
- More about how to tell whether someone is a private individual or a trader

Is a term allowed by law?

A term can't be unfair if it has to be included in a contract because the law says so. This might apply to some European Union legislation and international conventions. For example, information in your contract about the right to compensation from an airline if they've lost your possessions or if you've been injured.

Even if a term must be in the contract by law, it must still reflect the law accurately and not be misleading; otherwise you'd still be able to challenge it as being unfair.

What is the effect of an unfair term?

- Even if a contract term is unfair, the rest of the contract is normally valid unless the contract is unworkable without that term.
- The trader can't use an unfair term against you. For example, if a term says that a trader isn't responsible for faulty goods, they can't use this as a Defense if you take them to court for selling you faulty goods.

What can you do if you think a term is unfair?

- If you think a contract term is unfair, you should complain to the trader. If the trader doesn't agree, you should get advice before breaking the terms of the contract. You can get advice from the Citizens Advice consumer helpline who can report the trader to Trading Standards and other enforcement organizations.
- As a last resort you could take the trader to court and the court will decide whether a term is unfair. If a court decides that a term is unfair you could ignore the term or even cancel your contract and not pay a cancellation fee.

Unfair terms in contracts with traders in other EU countries

- If you buy goods or services from a trader in the European Union (EU), your rights around unfair contract terms will be very similar to those you have with a UK seller. If you believe a seller or supplier in another EU country has used an unfair term in their contract, you can complain.

What is consumer contract?

- A contract is an agreement between two or more people that is enforceable by law. When you buy goods or services you enter into a contract with the supplier of goods and services. This is called a consumer contract. Specifically a consumer is a person who is buying a service or a product from someone whose normal business it is to sell that product or service.
- Contracts may be written or oral. It is easier to know precisely what the terms are in a written contract but an oral contract is also enforceable in law. Consumer contracts may differ and there are no hard and fast rules governing what terms should be in a consumer contract.
- Contracts are made up of terms and there are different types of terms in consumer contracts. Implied terms are not mentioned in a written or oral consumer contract but exist all the same. An example of an implied term might be that the product or service will last for a reasonable length of time taking the cost of the item or service into account. Mandatory terms are terms that by law have to be included in contracts – these are not common in consumer contracts. Core terms are terms that set out the main conditions of a contract. In a consumer contract, these core terms might include the price of the product or service. Neither core terms nor mandatory terms are covered by the EU Unfair Terms in Consumer Contracts Regulation 1995.these regulations take into account the circumstances surrounding the conclusion of the contract. For example, whether the product or service was sold to the consumer in a fair and equitable manner.

- The regulations do not however, apply to any term that has been individually negotiated in a contract between a consumer and a supplier of goods and services. They also do not cover contracts between individuals selling products or services outside the course of their normal business or between one trader and another. Other contracts relating to employment, succession rights, family law or the formation of companies or partnerships are not covered by the regulations.

RBI ATM

An automated teller machine or automatic teller (ATM)
An Automated teller machine

ATM, American, Australian, Singaporean, Indian, Maldivian, Hibernoand Sri Lankan English), also known as an automated banking machine (ABM, Canadian English), cash machine, cashpoint,cashline, or colloquially hole in the wall (British and South African English), is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions without the need for a human cashier, clerk or bank teller.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date or CVVC (CVV). Authentication is provided by the customer entering a personal identification number (PIN).

Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated the money will be converted at an official exchange rate. Thus, ATMs often provide the best possible exchange rates for foreign travelers, and are widely used for this purpose

Many people have a habit of withdrawing small amounts of money from the ATM to curb spending tendencies, but often end up with a high frequency of withdrawals. There are some others who are reluctant to use net banking or mobile banking facilities and depend on ATMs for checking account balance. If you happen to fall into any of these categories, it's time to change your habit for good as RBI has issued new rules and guidelines limiting the number of times you use your ATM in a month. The new ATM transaction rules issued by the Reserve Bank of India is applicable to all ATM transactions including withdrawing cash, checking account balance or getting a mini account statement.

New RBI ATM Transaction Rules:

According to the new RBI guidelines that come into effect from 1st November 2014, savings bank account holders in metropolitan cities would be allowed only three transactions from ATMs of other banks and five from the same bank in a month. For any ATM transaction above the stipulated limit, a transaction fee of Rs. 20 would be charged to the account holder. The new transaction fee is applicable only for people living in six metropolitan cities including Mumbai, Delhi, Bangalore, Chennai, Hyderabad and Kolkata. People living in smaller towns and other centers would continue to enjoy five free monthly transactions per month from the ATM of other banks and the charges for them include Rs. 20 for each cash withdrawal and Rs 9 for non-cash transactions. Account holders of zero balance and other no-frills accounts in non metros are exempted from such transaction charges as of now.

What new Rules Mean for Bank Customers:

The transaction fee has been increased from the earlier limit of Rs. 15 and the number of free transactions decreased from five to three for ATMs of other banks. Another important change in the new RBI guideline policy for ATM transaction fee is the fact that all ATM transactions including cash

withdrawal, balance enquiry and changing of PIN number etc would be considered as an ATM transaction unlike in the past when balance enquiry was not considered a transaction as such!

A Case for Capping ATM Transaction Limit:

While capping the charges for ATM usage may be an unpopular decision taken by the Reserve Bank of India, the limit in free transactions is justified by the apex body considering high expenses for managing ATMs across the country. With an increasing number of robbery attempts on various ATMs especially in isolated areas and in semi urban and rural areas, the banks have been forced to shell out funds to install a security mechanism apart from using CCTVs and manual security guards wherever possible.

With the Reserve Bank of India laying down strict security guidelines not to leave any ATM unmanned or without security cameras and other measures, banks are facing higher overheads to manage the ATMs.

The inter banking fee charged by various banks through ATM services will also increase since banks are using the fee as an incentive to install more number of ATM machines. While all the above reasons have played their role in the decision to some extent the game clincher has been Reserve Bank of India's long term plan to promote the use of e-transfers and cashless transactions as much as possible to avoid the use of any black money in the system. The rise in ATM transaction fee is largely seen by financial experts as a sum culmination of all of the above factors.

Tips to bypass ATM Usage Limit:

Since the new RBI rules on ATM transaction limits are likely to affect a vast majority of people, here are some tips individual account holders can use to avoid the fee hike.

- **Avoid cash transactions whenever possible:** If you are one of those individuals using cash transactions for every purchase and other financial transactions, it is time to explore other ways. The use of electronic funds transfer, credit and debit cards, cheques and demand drafts must be explored for financial transactions than using cash all the time.
- **Change the habit of withdrawing smaller amounts:** With an increase in the ATM transaction fee make sure you avoid withdrawing small multiple amounts.
- **Visit bank branch for cash withdrawals:** If withdrawing large amount of cash, you are better off visiting the bank branch rather than the ATM. Visiting the bank branch may be slightly inconvenient, but it is a good idea to visit the bank branch to avoid the ATM transaction fee. Having said that, if this type of transaction happens once in a while, no harm in paying the charge versus waiting for your turn at the bank, if that is indeed the case.
- **Use online banking for statement:** A lot of people use ATMs for checking their account statement or to get a print of recent transactions or mini statement. Since ATM transactions count the number of visits even if it was for checking of account statement and not cash withdrawal, it is a good idea to use the internet banking facility for checking of account statement rather than the ATM machine.

A comparison of ATM usage charges:

For people living in metropolitan cities including Mumbai, Delhi, Bengaluru, Chennai, Hyderabad and Kolkata:

Bank	Transaction Type	Transaction Limit
Same Bank	• Cash Withdrawal • Balance Enquiry • Change of PIN • Mini Statement	5 free transactions per month. Additional transaction will be charged at Rs. 20 per transaction.
Different Bank	• Cash Withdrawal • Balance Enquiry • Change of PIN	3 free transactions per month. Additional transaction will be charged at Rs. 20 per transaction.

	• Mini Statement		
For people living in non metropolitan cities, smaller towns and holders of zero balance and other no-frills accounts:			
Bank	Transaction Type		Transaction Limit
Same Bank	• Cash • Balance Enquiry • Change of PIN • Mini Statement	Withdrawal	5 free transactions per months. 20 are applicable for each cash withdrawal and Rs 9 for non-cash transactions.
Different Bank	• Cash • Balance Enquiry • Change of PIN • Mini Statement	Withdrawal	5 free transactions per month. Rs. 20 is applicable for each cash withdrawal and Rs 9 for non-cash transactions. Charged at Rs. 20 per transaction.

The number of Automated Teller Machines (ATMs), which stood at a little over 27,000 as at end-March 2007, has increased to over 1.6 lakh across the country by end-March 2014. During the same period, the Point-of-Sale (POS) infrastructure has increased from 3.2 lakh to 10.65 lakh terminals. The ATMs are being gradually leveraged by banks to deliver other financial and non-financial products to their customers. Meanwhile, White Label ATMs (WLAs) have also been introduced in the country with the objective of increasing the ATM density and also building the rural and semi-urban ATM infrastructure. However, despite this growth, the deployment of both ATMs as well as POS infrastructure in the country is lop-sided with a significantly large presence in metropolitan and urban areas as compared to rural and semi-urban areas.

2. Recently, a few banks and the Indian Banks' Association (IBA) had approached the Reserve Bank seeking changes in the extant instructions regarding free transactions at other banks' ATMs. Referring to the growing cost of ATM deployment and maintenance incurred by banks on the one hand as well as the rising interchange out-go due to these free transactions, the IBA had sought the removal of free transactions at other banks' ATMs at metro centres and other large townships in the country.

3. In this regard, we draw attention to our circular DPSS No. 1405/02.10.02/2007-2008 dated March 10, 2008 as well as IBA circular No. CE.RB-1/atm/1284 dated August 31, 2009 on levy of service charges for use of ATMs. Reference is also invited to our circular DPSS.PD.No. 2632/02.10.002/2010-2011 dated May 27, 2011 which, inter alia, state that five free transactions per month (inclusive of financial and non-financial transactions) is permitted at other bank ATMs.

4. After an analysis of the ATM deployment in the country as well as availability of alternate means of electronic payment infrastructure and access thereto, it has been decided to revise the existing directions as under:[26]

a. Taking into account the high density of ATMs, bank branches and alternate modes of payment available to the customers, the number of mandatory free ATM transactions for savings bank account customers at other banks' ATMs is reduced from the present five to three transactions per month (inclusive of both financial and non-financial transactions) for transactions done at the ATMs located in the six metro centers, viz. Mumbai, New Delhi, Chennai, Kolkata, Bengaluru and Hyderabad. Nothing, however, precludes a bank from offering more than three free transactions at other bank ATMs to its account holders if it so desires.

b. This reduction will, however, not apply to small / no frills / Basic Savings Bank Deposit account holders who will continue to enjoy five free transactions, as hitherto.

c. At other locations i.e. other than the six metro centers mentioned above, the present facility of five free transactions for savings bank account customers shall remain unchanged.

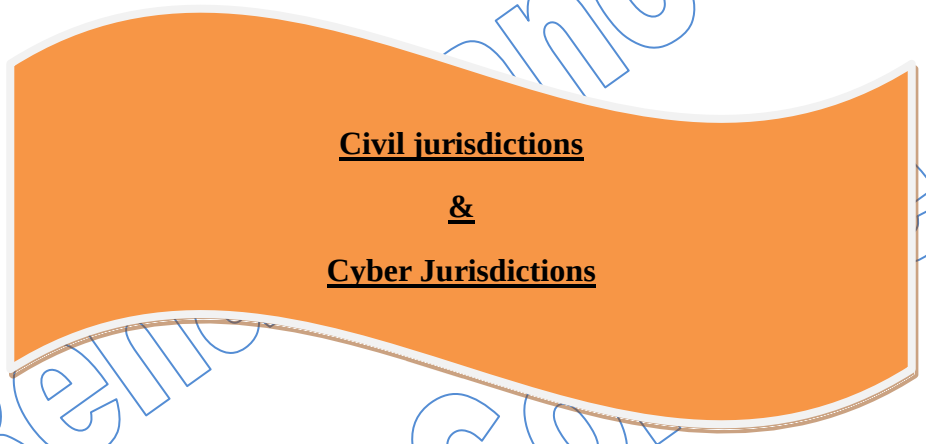
[26] http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=9170&Mode=0

d. ATM installing banks are advised to indicate clearly at each ATM location that the ATM is situated in a 'metro' or 'non-metro' location using appropriate means (message displayed on the ATM / sticker / poster, etc.) to enable the customer to identify the status of the ATM in relation to availability of number of free transactions. Further, banks are advised to ensure the "ATM location identifiers" in their ATM database is accurate and kept up-to-date at all times so as to minimize disputes, if any, in the matter.
e. The issuing banks are also advised to put in place proper mechanisms to track such transactions and ensure that no customer inconvenience or complaints arise on this account.
f. The provisions related to levy of charges for use of own-bank ATMs, vide our circular dated March 10, 2008, has also been reviewed. Accordingly, banks are advised that at least five free transactions (inclusive of financial and non financial transactions) per month should be permitted to the savings bank account customers for use of own bank ATMs at all locations. Beyond this, banks may put in place appropriate Board approved policy relating to charges for customers for use of own bank ATMs.
g. The ceiling / cap on customer charges of Rs.20/- per transaction (plus service tax, if any) will be applicable.
h. Banks are advised to ensure that the charges structure on ATM transactions, as per their Board approved policy, is informed to the customer in a fair and transparent manner.
i. Further, banks are advised to put in place suitable mechanism for cautioning / advising / alerting the customers about the number of free transactions (OFF-US as well as ON-US) already utilized during the month by the customer and the possibility that charges may be levied as per the banks' policy on charges.

UNIT-4

INTERNATIONAL AT SPHERE OF GLOBAL REGIME

1	**Civil Jurisdictions**
2	Minimum contact Doctrine in U.S.A.
3	E mail on Internet
4	Danger for computer software failure



The internet can be seen as a multi jurisdictional because of the ease which a user can access of website anywhere in the world. It can be even viewed as a jurisdictional in the sense that from the user's perspective that the state and national borders are essentially transparent. For courts determining jurisdiction situation is more problematic. The court in *Zippo mfg. v. Zippo dot com inc* said that there is a global revolution looming on the horizon and the development of the law in dealing with the allowable scope of personal jurisdiction based on internet use in its infancy

The developing law of jurisdiction must addressed whether a particular event in cyber space is controlled by the law of state or country where the website is located, by the law of the state or the country where the internet service provider is located. A number of commentators have voiced their opinion that cyber space should be treated as separate jurisdiction. In practice this view has not been supported or addressed by the law makers. Cyber jurisdictional cases have been dealt with primarily in civil courts. *Since the advent of US v. Thomas, infra and Minnesota v. Granite gate resort.*

Cyber jurisdictions issues have been began to be examined in criminal courts as well.

- Cyber Jurisdiction in Criminal Cases: - the question of cyber jurisdiction came to a forefront of attention of early 1996 in US. v. Thomas where the sixth circuit upheld the conviction of a couple operating a pornographic bulletin from their home.
- The AABBS content approximately 14000 gif files. These files should be easily accessed or retrieved or download by one who possessed a password. 1994, a US magistrate judge issued a search warrant which led to authorizing the confiscation of the defendant computers. The defendant was convicted in the district courts against which they appealed. The court held that the statute must be construed to affect the intent of the Congress which was to prevent any obscene matter. —D argued that the internet environment provides broad ranging connections

among people in cyberspace. As such that notion obscenity tied to geographical local would put a chill on protected speech.

- 'D'asserted a more flexible definition was needed was DMS operator could not select to receive their materials.
- The court ruled out that the D had pre existing method of screening potential members by pre-screening their members; they could protect themselves from being subjected to liability in jurisdiction with less tolerant standards. This could be further said that D was to tailor their message on as selective to the communities it should to serve so there no need to develop any definition.

Liability of Internet Services Provider

Internet service Providers acts a link for the activities that takes place on the internet. He runs the risk of being liable for information that is transmitted over the information system provide by his services. S.79 of I.T. Ct, 200 provides the network service providers is not subject to any civil or criminal liability under this act for any third party information or data made available by him, if, he proves that the offence was committed without his knowledge., or that he had exercised all due diligence to prevent the commissioning of such offence. NSPs will be held liable for their consent or third party consent that they adopt or approve of.

With transactions occurring over an open network environment, questions are raised as to the liability of the carriers of their transactions, disputes and problems arise. In the physical world, intermediaries such as publishers for the content published by the authors. However, in the electronic there are some classes of intermediaries who carry the data and do not exercise the direct control over the content. For promoting the electronic transaction it is important to clarify the liability if such NSPs. It is proposed that intermediaries who are ISPs are not responsible for thirds party content for which they mere provide access to. It is necessary to insure that providers do not shirk their responsibilities under the licensing scheme to regulate the undesirable content. The provision therefore makes it clears that it will absolve ISPs from their licensing obligations.

1. **Minimum contacts**

Minimum contacts is a term used in the United States law of civil procedure to determine when it is appropriate for a court in onestate to assert personal jurisdiction over a defendant from another state. The United States Supreme Court has decided a number of cases that have established and refined the principle that it is unfair for a court to assert jurisdiction over a party unless that party's contacts with the state in which that court sits are such that the party "could reasonably expect to be haled into court" in that state. This jurisdiction must "not offend traditional notions of fair play and substantial justice". A non-resident defendant has minimum contacts with the forum state if they 1) have direct contact with the state; 2) have a contract with a resident of the state;3) have placed their product into the stream of commerce such that it reaches the forum state; 4) seek to serve residents of the forum state; 5) have satisfied the Calder effects test; or 6) have a non-passive website viewed within the forum state.

Introduction

In Personam Jurisdiction refers to the power which a court has over the defendant himself in contrast to the court's power over the defendant's interest in property (Quasi in rem) or power over the property itself (in rem)[27]. A court that lacks personal jurisdiction is without power to issue an in personam judgment i.e. judgment against the individual or corporation. The Minimum Contact theory

[27] *Black's Law Dictionary, (6th Ed.) p.790*

comes into picture when either or both of the parties seem to be from outside the Court's territorial jurisdiction. It is used as a method to establish the Court's jurisdiction over the parties to a case by determining their quality and intensity of their contact i.e. services or transactions with the Forum State. In India, it has been incorporated by giving a liberal interpretation to *Section 20(c) of the Code of Civil Procedure*, to expand jurisdiction especially in cases of trademark infringement, passing off of trademarks, domain name infringements.

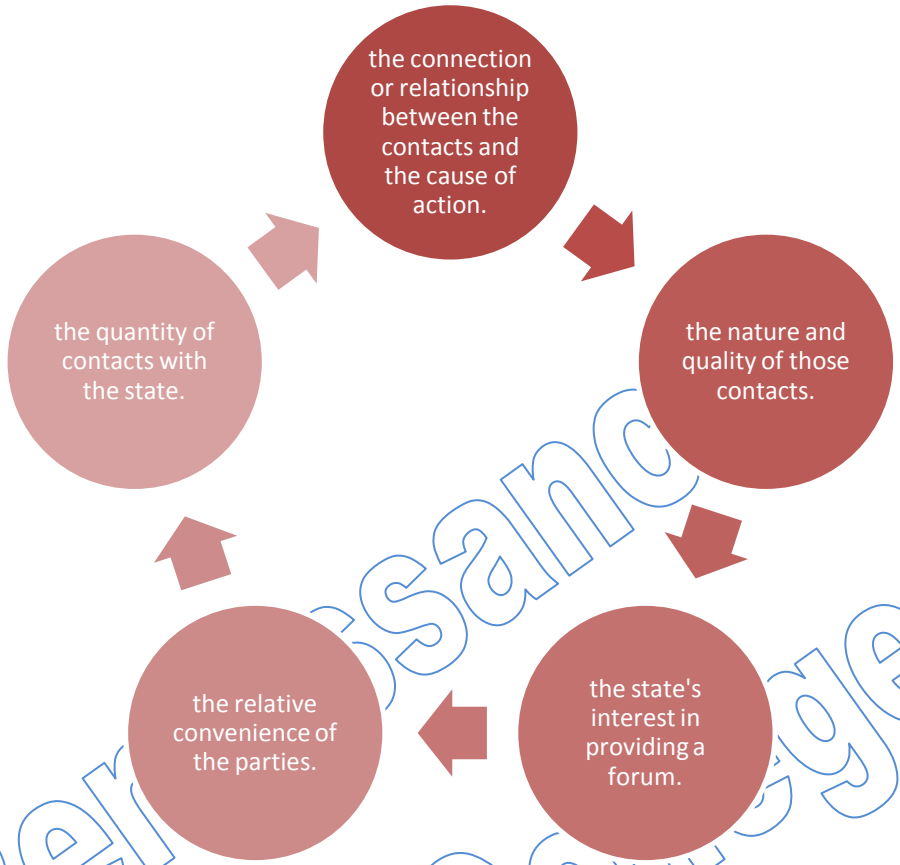
Origin of the theory

In America, concept of personal jurisdiction and fairness and due process were not on the same page traditionally. Non-residents could be brought to court while they were in State, however fortuitous or brief presence it might be. With the *International Shoe v. Washington*[28], modern jurisdictional analysis stepped in, imbibing Fair play and substantial justice in exercising of personal jurisdiction by courts. Incorporating the spirit of the Fourth and Fifteenth Amendments to the United States Constitution that talk about substantive due process and procedural due process, the core meaning of due process of law is to secure the principle of legality by ensuring that executive and judicial deprivations are grounded in valid legal authority. In this case, a suit to recover payments due to the unemployment fund by a Corporation which did not even have an office or shop in the State was questioned on the basis of personal jurisdiction. Service of process upon one of the corporation's salesmen within the State, and notice being sent by registered mail to the corporation at its home office was challenged as not satisfying the requirements of due process[8]. The Supreme Court of Washington was of opinion that the regular and systematic solicitation of orders in the state by appellant's salesmen, resulting in a continuous flow of appellant's product into the state, was sufficient to constitute doing business in the state so as to make appellant amenable to suit in its courts.

Earlier the parties' presence within the territorial jurisdiction of a court was prerequisite to its rendition of a judgment personally binding him[9]. Later the position developed that due process required only that, in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice"[10]. It was held*supra*, that, to the extent that a corporation exercises the privilege of conducting activities within the State, it enjoys the benefits and protection of laws of the State and obligations arising out of these which require the Corporation to respond to a suit brought to enforce them can, in most instances, will be held binding on it. Hence, the Corporation is bound by its purposeful availment in that forum.

Some of the factors which may be examined, among others, to determine whether minimum contacts exist include:

[28] *326 U.S. 310, 1945*



Development of the theory in the International arena

Shoe (*Supra*) lay down that Courts could exercise general personal jurisdiction as well as specific personal jurisdiction, depending on the level of contact. If contact is so continuous and substantial that the subject can be sued for anything within the State, it's the former, but if the contact is only sufficient for jurisdiction over claim arising from those contracts, it's the latter. With the development of Internet and globalization of business, businesses spread worldwide had the risk of being sued anywhere, which mandated stricter norms in determining "Purposeful Availment", also known as *Sliding Scale test*. The case of *Asahi Metal Industry Co. v. Superior Court* questioned if the mere awareness that a product may reach a remote jurisdiction when put in the stream of commerce was sufficient to satisfy the requirement for minimum contacts under the Due Process Clause. The courts here and in *World-Wide Volkswagen Corp. v. Woodson* held that a party must do more than intentionally put goods in the stream of commerce even if it expected its products to reach the forum state. Foresight alone wasn't enough to establish personal jurisdiction over the defendant Corporations here as neither party deliberately took steps to see their products in the forum markets. The substantial connection with the forum state necessary for a finding of minimum contacts must come about by an action of the defendant purposefully directed toward the forum state. Even after that, fair play and justice will have to be satisfied i.e. reasonableness of the party to be sued in that forum.

The cases of *Cybersell Inc v. Cybersell Inc and Ors and Chloe v. Queen Bee of Beverly Hills, LLC* gave a three step test to exercise personal jurisdiction in matters dicey in territorial jurisdiction.

1. The nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws.
2. The claim must be one that arises out of or results from the defendant's forum related activities.
3. Exercise of jurisdiction must be reasonable

But the case of *Panavision International LP* brought out the loophole in application of existing rules of personal jurisdiction to conduct that took place in part in cyberspace - it was observed that simply registering someone else's trademark as a domain name and posting a website on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another. Even a passive website cannot be the subject of a Court's personal jurisdiction, until it harms the other. The Minimum Contact Theory wasn't sufficient to determine such cases wherein the level of contact or interactivity of the domains couldn't be defined. This brought in the aspect of 'active intention of the party to establish contact with the forum state, economically benefit itself and harm the interests of the plaintiff by targeting the latter's market. It led to the development of Calder test (effect test) i.e. exercising jurisdiction by objective territoriality.

In the case of *Burger King Corp v. Rudzewicz*, it was held that the court could exercise jurisdiction over a nonresident despite his physical absence, where an alleged injury arises out of or relates to actions by the Defendant himself that are "purposefully directed towards residents of the forum State". It was also held that "purposeful availment" would not result from "random" or "fortuitous" contacts by the defendant in the forum state, the plaintiff was required to show that such contacts resulted from the "actions by the defendant himself that created a substantial connection with the forum State" i.e. he must have engaged in "significant activities" within the forum state or have created "continuing obligations" between himself and residents of the forum state.

Summarizing the position in the US, to establish personal jurisdiction of the Court, even when a long arm statute existed and Effects test proved, plaintiff would have to show that the defendant purposefully availed of jurisdiction of the forum state by "specifically targeting" customers within the forum state.

In England, until the passive display is advertisement, it wouldn't be viewed as targeting. Countries like Australia and Canada are supported by their long-arm statute, which though decreases the importance of Minimum Contact theory, doesn't diminish the importance of due process requirements, including reasonability. Reasonableness of exercise of jurisdiction can be gauged by considering the following measures- the burden on the defendant of coming for a trial in that forum state, the interests of the forum State, the plaintiffs interest in obtaining relief, the interstate judicial system's interest in obtaining the most efficient resolution of controversies and the shared interest of the several States in furthering fundamental substantive social policies

Use in India

As the businesses in India are extending their horizons globally hence the use of Minimum Contact Theory was used to expand jurisdiction of Courts in cases trademark infringement through domain name and when some non-residents are involved. In the case of *(India TV) Independent News Service Pvt Limited Vs. India Broadcast Live LLC and Ors and Banyan Tree Holding (P) Limited vs. A. Murali Krishna Reddy and Anr.*, the foreign precedents were rushed to provide the justification for exercising jurisdiction over the defendants. As jurisdiction in our courts is defined by territorial and pecuniary jurisdiction, a liberal interpretation of Section 20(c) of Code of Civil Procedure by the Courts allowed this.

In India TV case, the court established minimum contact of the defendant with the forum state to exercise jurisdiction. It was found out that the website could not only be accessed from but also subscribed to from Delhi and it was thus contended that the defendant was carrying on business with deliberative effort for profit or gain from India. As the plaintiff was a corporation based in India in the

same field, its economic interests were being hampered. Hence, according to the Cybersell case, court held that defendant in this case had directed his activity toward the forum state i.e. Delhi and held defendant liable for passing off.

In Banyan Tree case, it was held that creating a site, was like placing a product into the stream of commerce, which may be felt nationwide or even worldwide but, without more, it was not an act purposefully directed towards the forum state". Purposeful Availment means that it has to be actively intentional. The Courts in order to ensure that this method of exercising jurisdiction didn't violate the codified method of territorial jurisdiction, the Courts, in both these cases used Section 20(c) of the Code of Civil Procedure, i.e. the case can be instituted where the cause of action arises. Courts held that even if neither the plaintiff, nor the defendant were within the local jurisdiction of the Court where the case was instituted, but it was proved that the domains of the defendant were accessed by the people belonging to the plaintiff's market under the impression of the defendant being the plaintiff, because of similar trademarks or domain names, then cause of action will deemed to have arisen in that market and the case could be instituted there. Mere avoidance to restrict the access of their sites outside the defendant's local jurisdiction could not be an excuse if people would take services from it, thus harming the other similar Corporation.

Danger to Computer failure

It is common to use programmable computers in applications where their failure could be life threatening and could result in extensive damage. When computers are used to replace electromechanical devices that can achieves higher reliability levels, then safety may even be impaired. Even when computers can improves safety, it is not clear that the end result is actually an increase in system safety. Despite potential problems, however, computers are being introduced to control some hazardous systems. The majority of people using these computers believe that these programmable computers never fail and whatever comes out of them has to be taken for granted. It is likely that typical programmers leave around 50 errors per thousand lines of code that they write; Software errors do not have serious sequences because people can repair the damage at some cost in time and aggravation, but some products do not provide much opportunity for people to correct errors. When a computer controls a linear accelerator or an airplane, the results of an error cannot be discarded or ignored. If the patient dies or the airplane crashes, the computation cannot be "done over". Applying typical programming practices to critical systems like these can result in tragedy.

Examples of Computer Failure

Incidents of failures of computers are not all the same. We begin by given some of the incidents which caused inconvenience and then move to more serious examples involving Financial, Aviation, and Medical systems which cause loss of money and or human lives.

- January 1998 news reports told of software problems at a major U.S. telecommunications company that resulted in no charges for long distance calls for a month for 400,000 customers. The problem went undetected until customers called up with questions about their bills.
- In November of 1996, newspapers reported that software bugs caused the 411 telephone information system of one of the U.S. RBOC's to fail for most of a day. Most of the 2000 operators had to search through phone books instead of using their 13,000,000-listing database. The bugs were introduced by new software modifications and the problem software had been installed on both the production and backup systems. A spokesman for the software vendor reportedly stated that 'It had nothing to do with the integrity of the software. It was human error.

1 Examples of Financial system Failure

There are so many incidents related to computer software in the financial industry. Here are some examples:

-Due to a bank error in the exchange rate, an Australian man was able to purchase Sri Lanka rupees for (Australian $ 104,500 and then sell them to another bank the next day for $ 440,258. (The first bank's computer had displayed the Central Pacific France rate in the rupee position.) Because of the circumstances surrounding the bank's error, a judge ruled that the man had acted without intended fraud, and could keep his windfall of $ 335,758.

Examples of Aviation system Failures

There are so many incidents related to computer software in the aviation industry. The ideal model that we will investigate closely is the European Airbus 320 which uses the computer software to control all activities of the aircraft.

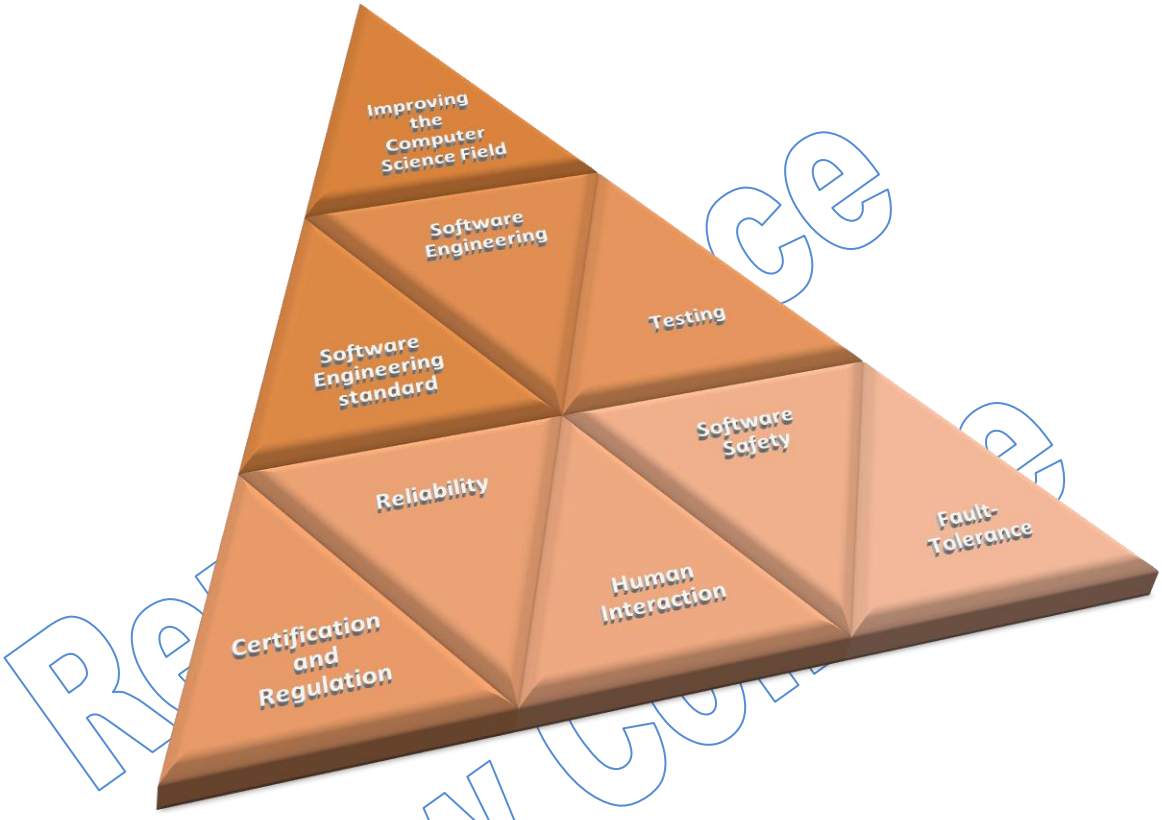
-The 125 million dollar Mars Climate Orbiter is assumed lost by officials at NASA. The failure responsible for loss of the orbiter is attributed to a failure of NASA's system engineer process. The process did not specify the system of measurement to be used on the project. As a result, one of the development teams used Imperial measurement while the other used the metric system of measurement. When parameters from one module were passed to another during orbit navigation correct, no conversion was performed, resulting in the loss of the craft

Examples of Medical system failures

Use of computerized devices will continue to enable new clinical procedures and functions to be performed, ones that could not have been done by a team of medical experts without the aid of automation. In addition, the reliability and relative safety of procedures performed by computerized devices should generally be higher than manually-performed, labor-intensive, tasks. Under manual operation, users are prone to occasional inattention, fatigue or boredom, which lead to human error. This can compromise patient safety. However, safety and clinical effectiveness can also be compromised in automated systems if attention to "computer safety" and/or Quality Assurance (QA) procedures are not used in the design, manufacture, testing and Installation of these automated devices.

Minimizing the Risks of Failure

To following factors may reduce the risk and danger of computer software failure



Improving the Computer Science Field

In the US and around the world, Computer Science academic programs award high number of Bachelor of Science (BS), Master of Science (MS) degrees annually. Some of these students enter Ph.D. Many of these graduates take computing jobs for which they are inadequately educated, such as helping to develop high performance computing applications to improve the performance of human organizations. The programming profession includes a great range of education and abilities, and many curricula should provide instruction in topics relevant to building safe systems. Studies of employed programmers have found that the best can be more than 25 times as capable as the worst and some teams out produce others by factors of four or five

Software Engineering

Producing quality software is largely a design and management problem, not a coding problem. Individual programmers usually comprehend their creations at the level of modules that are most a few hundred lines long. Most programmers are trained to concentrates on this level. Building large programs that are tens of thousands of lines long requires a different set of skills.

Emphasizing communication and organization in order to extract useful specifications, divide the project into modules that are reasonable work. The central idea of software engineering is that programming projects have to be performed in stages, with an identifiable end product at each state. The final product is the program itself. There are several or many; intermediate stages are documents about the program. Typically, these include a specification describing what the product is supposed to

do. A design guide describing how the program is organized, a plan describing a series of tests that are supposed to show that the program works as promised in the specification and a test report that presents the test results and explains how any problems were resolved. This enforces an orderly development process, makes progress visible to management, and enables products to be reviewed by experts other than their creators. Programmers ought to work much differently on engineered software projects. Their effort has to be devoted to planning and design, and much of the rest goes for testing and quality assurance. Only 15% to 20% must be spent on coding statements in a programming language without this guidance, skilled coders flounder. The all-too- frequent result is programs that seem to work, but then fail unexpectedly. It's extremely hard to build a large computer program that works correctly under all required conditions, but it's easy to build one that works 90 percent of the time. The following measures if followed will reduce the number of bugs in the software; however, it will not guarantee that the software is 100% correct:

A) Documentation should not be an afterthought.

Software quality assurance practices and standard should be established.

B) Designs should be kept simple.

C) Ways to get information about errors, i.e., software audit trails, should be designed into the software from the beginning.

D) The software should be subjected to extensive testing and formal analysis at the module and software level; system testing alone is not adequate

Software Engineering standard

The whole purpose of staged development is to ensure that the necessary planning and design is performed. There exist many so-called software standards that are actually, documentation standard that describe the format of the documents in considerable detail. The fact that the standards define only what the reports must look like but not what programmers must do explain the disappointment that most programmers feel when they first read them. Conscientious programming teams usually develop their own documentation style, which is well-matched to their product and their favored design methods.

Certification and Regulation

We regulate product that have safety implications: building, bridges, airplanes, drugs. The government established standards that these products must meet and conduct inspections to make sure products comply. We also must regulate people that provide safety critical services: they must satisfy educational requirements and examinations. Software is still largely unregulated. Until recently, aviation and nuclear power were the only applications in which software purchased or operated by private enterprise was subject to approval by the government.

Testing

Most programmers are not able to demonstrate that their programs will compute the intended results, except by running tests. It is literally a trial-and error process. It is not terribly confidence-inspiring because the number of possible situations that a program must deal with is usually much too large to test, and a case that was left out of the test set may cause the program to fail. As result, errors are left in products to be discovered when they reach the market. They are corrected over time as the system is used. Testing should be performed with balance between safety and cost

Fault-Tolerance

If the application produced is used in a critical system where human lives are at risk, and if it is economically affordable to use Fault Tolerant technique such as N-Version programming (where different programs written independently from the same specification, and then executing them in parallel, with conflicts resolved by majority voting) should be done after intensive studying. This may

reduce the problem. Although, it has been shown, that even when the different versions appear to be independent, they may exhibit common fault modes or have logically related flaws.

Reliability

Formal methods are mathematically base techniques for increasing product reliability that overcome some of the limitations of trial-and-error testing. Computer scientists have been pursuing formal methods for more than 30 years, but they are almost never used in practice. Although, the techniques are so difficult and cumbersome, it should be applied to programs.

Software Safety

Safety-critical products demand a different, more rigorous approach than most other computer applications. They require several disciplines that should be familiar to many programmers and programming managers: safety engineering teaches how to design systems that remains safe even when hardware or software fails. The most important lesson of safety engineering is that safety is an important system requirement in its own right and must be designed into a product, not added on as an afterthought. Safety requirements often inflate with other system requirements and may suggest a quite different design than would be detained if cost and performance were the only considerations. Resolving such conflicts in a consistent manner demands that safety requirements be explicitly separated out and that responsibility for meeting them be assigned to someone with authority. A safe system protects from hazards whether its intended functions performed correctly or not. In fact, safety is most concerned with what happens when the system does not work as expected. Safety engineers assume that systems will fail and then they work through the consequences.

Human Interaction

Facing all the risks of computers does not mean that such systems should not be built and used, only that we need to understand when they can be useful and when can be dangerous and to design them very carefully according to principles of cognitive psychology. It may be easier to change the way the systems are designed than to try to change human nature. The important choice may not be between using such systems or not using them but between building them with or without careful consideration of the humans who will be interacting with them. If we do not yet know enough about the way that human interact with machines, then perhaps this is as important a research topic as studying the technological aspects of design

EMAIL ON INTERNET

Electronic mail, most commonly referred to as email or e-mail since c 1993, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to a mail server, for as long as it takes to send or receive messages. Historically, the term electronic mail was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to describe fax document transmission. As a result, it is difficult to find the first citation for the use of the term with the more specific meaning it has today.

An Internet email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

Electronic mail predates the inception of the Internet and was in fact a crucial tool in creating it, but the history of modern, global Internet email services reaches back to the early ARPANET[29]. Standards for encoding email messages were proposed as early as 1973 (RFC 561). Conversion from ARPANET[30] to the Internet in the early 1980s produced the core of the current services. An email message sent in the early 1970s looks quite similar to a basic text message sent on the Internet today.

Email is an information and communications technology. It uses technology to communicate a digital message over the Internet. Users use email differently, based on how they think about it. There are many software platforms available to send and receive. Popular email platforms include Gmail, Hotmail, Yahoo! Mail, Outlook, and many others.

[29] Advanced Research Projects Agency Network

[30] Experimental email transfers between separate computer systems began shortly after the creation of the ARPANET in 1969. Ray Tomlinson is generally credited as having sent the first email across a network, initiating the use of the "@" sign to separate the names of the user and the user's machine in 1971, when he sent a message from one Digital Equipment Corporation DEC-10 computer to another DEC-10. The two machines were placed next to each other. Tomlinson's work was quickly adopted across the ARPANET, which significantly increased the popularity of email. For many years, email was the killer app of the ARPANET and then the Internet.

UNIT-5
RIGHT TO PRIVACY(ON INTERNET)
MEDIA LAW

1	**Right to Privacy – Breach of (Defamation, Trespass, Nuisance)**
2	Breaching confidence and harassment
3	Privacy on Internet
4	Real Victims of Virtual Crime

Right to privacy- breach of (defamation, trespass and nuisance)

Freedom of Expression

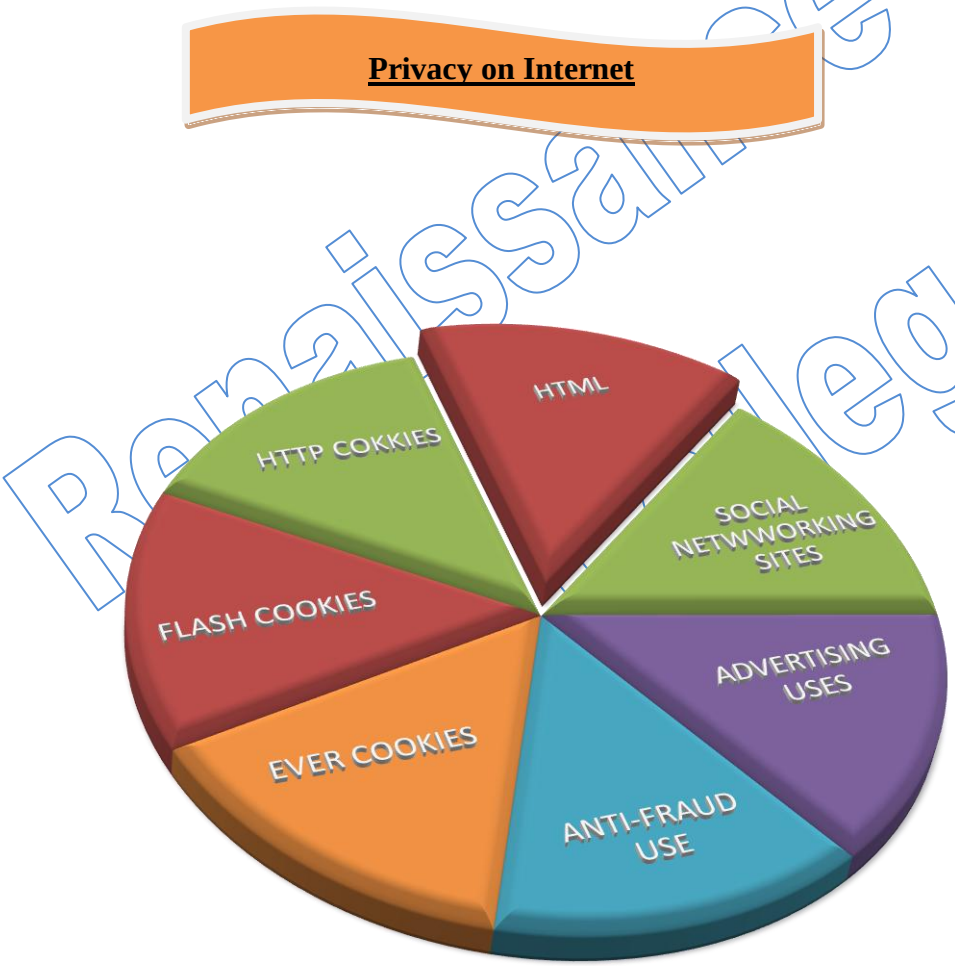
The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (Section 67B) has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc.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

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

Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Article 19(1)(a) of our Constitution. The fact that some information is "grossly offensive" (Section 66A (a)) or that it causes "annoyance" or "inconvenience" while being known to be false (Section 66A(c)) cannot be a reasons 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 Article 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 Section 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 Section 66A(c) to make clear what "origin" means in that section. Because depending on the construction of that word Section 66A(c) can, for instance, unintentionally prevent organizations from using proxy servers, and may prevent a person from using a sender envelope different form the "from" address in an e-mail (a feature that many e-mail providers like G-mail 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 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests is specified, no guidelines have been specified. Those guidelines, per Section 69A (2), "shall be such as may be prescribed". It has to be ensured that they are prescribed first, before any powers of censorship are granted to anybody. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable.



Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of computer privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing. Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behavior on a website. PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

Risk to internet privacy

Companies are hired to watch what internet sites people visit, and then use the information, for instance by sending advertising based on one's browsing history. There are many ways in which people can divulge their personal information, for instance by use of "social media" and by sending bank and credit card information to various websites. Moreover, directly observed behavior, such as browsing logs, search queries, or contents of the Facebook profile can be automatically processed to infer potentially more intrusive details about an individual, such as sexual orientation, political and religious views, race, substance use, intelligence, and personality. Those concerned about Internet privacy often cite a number of privacy risks — events that can compromise privacy — which may be encountered through Internet use. These range from the gathering of statistics on users to more malicious acts such as the spreading of spyware and the exploitation of various forms of bugs (software faults).Several social networking sites try to protect the personal information of their subscribers. On Facebook, for example, privacy settings are available to all registered users: they can block certain individuals from seeing their profile, they can choose their "friends", and they can limit who has access to one's pictures and videos. Privacy settings are also available on other social networking sites such as Google Plus and Twitter. The user can apply such settings when providing personal information on the internet.

HTTP cookies

An HTTP cookie is data stored on a user's computer that assists in automated access to websites or web features, or other state information required in complex web sites. It may also be used for user-tracking by storing special usage history data in a cookie, and such cookies—for example, those used by Google Analytics—are called tracking cookies. Cookies are a common concern in the field of Internet privacy. Although website developers most commonly use cookies for legitimate technical purposes, cases of abuse occur. In 2009, two researchers noted that social networking profiles could be connected to cookies, allowing the social networking profile to be connected to browsing habits.

In the past, web sites have not generally made the user explicitly aware of the storing of cookies, however tracking cookies and especially third-party tracking cookies are commonly used as ways to compile long-term records of individuals' browsing histories — a privacy concern that prompted European and US law makers to take action in 2011. Cookies can also have implications for computer forensics. In past years, most computer users were not completely aware of cookies, but recently, users have become conscious of possible detrimental effects of Internet cookies: a recent study done has shown that 58% of users have at least once, deleted cookies from their computer, and that 39% of users delete cookies from their computer every month. Since cookies are advertisers' main way of targeting potential customers, and some customers are deleting cookies, some advertisers started to use persistent Flash cookies and zombie cookies, but modern browsers and anti-malware software can now block or detect and remove such cookies. The original developers of cookies intended that only the website that originally distributed cookies to users could retrieve them, therefore returning only data already possessed by the website. However, in practice programmers can circumvent this restriction. Possible consequences include:

- the placing of a personally-identifiable tag in a browser to facilitate web profiling (see below), or,
- use of cross-site scripting or other techniques to steal information from a user's cookies.

Flash cookies

When some users choose to disable http cookies to reduce privacy risks as noted, new types of cookies were invented: since cookies are advertisers' main way of targeting potential customers, and some customers were deleting cookies, some advertisers started to use persistent Flash cookies and zombie cookies. In a 2009 study, Flash cookies were found to be a popular mechanism for storing data on the

top 100 most visited sites. Another 2011 study of social media found that, "Of the top 100 web sites, 31 had at least one overlap between HTTP and Flash cookies."[23] However, modern browsers and anti-malware software can now block or detect and remove such cookies. Flash cookies, also known as Local Shared Objects, work the same ways as normal cookies and are used by the Adobe Flash Player to store information at the user's computer. They exhibit a similar privacy risk as normal cookies, but are not as easily blocked, meaning that the option in most browsers to not accept cookies does not affect Flash cookies. One way to view and control them is with browser extensions or add-ons. Flash cookies are unlike HTTP cookies in a sense that they are not transferred from the client back to the server. Web browsers read and write these cookies and can track any data by web usage. Although browsers such as Internet Explorer 8 and Firefox 3 have added a 'Privacy Browsing' setting, they still allow Flash cookies to track the user and operate fully. However, the Flash player browser plug-in can be disabled or uninstalled, and Flash cookies can be disabled on a per-site or global basis. Adobe's Flash and (PDF) Reader are not the only browser plugging whose past security defects have allowed spyware or malware to be installed: there have also been problems with Oracle's Java.

Evercookies

Evercookies, created by Samy Kamkar, are JavaScript-based applications which produce cookies in a web browser that actively "resist" deletion by redundantly copying themselves in different forms on the user's machine (e.g., Flash Local Shared Objects, various HTML5 storage mechanisms, window.name caching, etc.), and resurrecting copies that are missing or expired. Evercookies accomplishes this by storing the cookie data in several types of storage mechanisms that are available on the local browser. It has the ability to store cookies in over ten types of storage mechanisms so that once they are on one's computer they will never be gone. Additionally, if ever cookie has found the user has removed any of the types of cookies in question; it recreates them using each mechanism available. Evercookies are one type of zombie cookie. However, modern browsers and anti-malware software can now block or detect and remove such cookies.

Anti-fraud uses

Some anti-fraud companies have realized the potential of Evercookies to protect against and catch cyber criminals. These companies already hide small files in several places on the perpetrator's computer but hackers can usually easily get rid of these. The advantage to Evercookies is that they resist deletion and can rebuild themselves.

Advertising uses

There is controversy over where the line should be drawn on the use of this technology. Cookies store unique identifiers on a person's computer that are used to predict what one wants. Many advertisement companies want to use this technology to track what their customers are looking at online. Evercookies enable advertisers to continue to track a customer regardless of if one deletes their cookies or not. Some companies are already using this technology but the ethics are still being widely debated.

Privacy issues of social networking sites

The advent of the Web 2.0 has caused social profiling and is a growing concern for Internet privacy. Web 2.0 is the system that facilitates participatory information sharing and collaboration on the Internet, in social networking media websites like Facebook, Instagram, and MySpace. These social networking sites have seen a boom in their popularity starting from the late 2000s. Through these websites many people are giving their personal information out on the internet.

It has been a topic of discussion of who is held accountable for the collection and distribution of personal information. Some will say that it is the fault of the social networks because they are the ones who are storing the vast amounts of information and data, but others claim that it is the users who are

responsible for the issue because it is the users themselves that provide the information in the first place. This relates to the ever-present issue of how society regards social media sites. There is a growing number of people that are discovering the risks of putting their personal information online and trusting a website to keep it private. Once information is online it is no longer completely private. It is an increasing risk because younger people are having easier internet access than ever before, therefore they put themselves in a position where it is all too easy for them to upload information, but they may not have the caution to consider how difficult it can be to take that information down once it is out in the open. This is becoming a bigger issue now that so much of society interacts online which was not the case fifteen years ago. In addition, because of the quickly evolving digital media arena, people's interpretation of privacy is evolving as well, and it is important to consider that when interacting online. New forms of social networking and digital media such as Instagram and Snap chat may call for new guidelines regarding privacy. What makes this difficult is the wide range of opinions surrounding the topic, so it is left mainly up to our judgment to respect other people's online privacy in some circumstances. Sometimes it may be necessary to take extra precautions in situations where somebody else may have a tighter view on privacy ethics. No matter the situation it is beneficial to know about the potential consequences and issues that can come from careless activity on social networks.

HTML

HTML5 is the latest version of Hypertext Markup Language specification. HTML defines how user agents, such as web browsers, are to present websites based upon their underlying code. This new web standard changes the way that users are affected by the internet and their privacy on the internet. HTML5 expands the number of methods given to a website to store information locally on a client as well as the amount of data that can be stored. As such, privacy risks are increased. For instance, merely erasing cookies may not be enough to remove potential tracking methods since data could be mirrored in web storage, another means of keeping information in a user's web browser. There are so many sources of data storage that it is challenging for web browsers to present sensible privacy settings. As the power of web standards increases, so do potential misuses.

Real victim of virtual crime

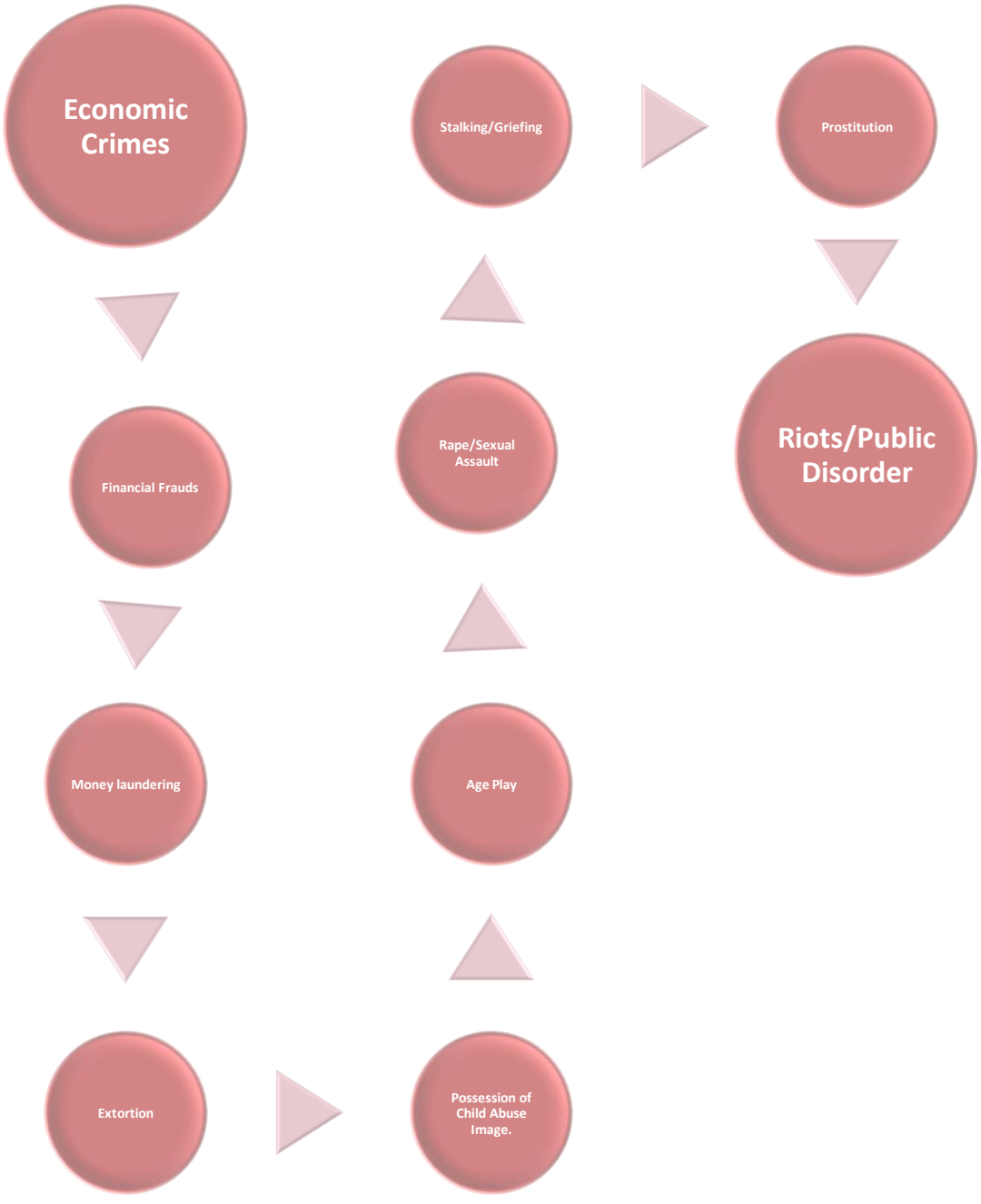
While there is extensive literature available on cybercrimes such as hacking, online child pornography, identity theft and cyber stalking relatively little academic literature has been published concerning crime in online virtual worlds. Regardless, several cases have come to light concerning specific crimes in online virtual worlds. These crimes have involved both property offences (such as theft) and crimes against the person (such as sexual assault).

Many police officials, including seasoned and experienced cybercrime investigators, may not have yet investigated a case involving a virtual world or MMORPG. Faced with already overwhelming caseloads from traditional forms of cybercrime, such as hacking, Internet fraud and online child abuse images, few investigators want additional work from virtual cases. That said, we believe that virtual world crimes merit further examination given their inevitable emergency into the daily workload of cybercrime investigators around the world.

While it might be tempting to ignore MMORPG[31] crimes as being purely virtual in nature, and thus not "real," the vast majority of virtual crimes have real world victims. While one can certainly argue

[31] Massive Multiplayer Online Role-Playing Games MMORPG's are videogames that allow thousands of players to simultaneously enter a virtual world and interact with one another. Players can run their own "cities and countries,"

whether "virtual rape" indeed constitutes "real rape," let there be no doubt about the economic or psychological effect of these crimes on their victims, since these virtual spaces are every bit as real to their inhabitants as is the physical world to most investigators.



stand up armies to win battles and go on any variety of "quests" with their own avatars. These avatars are completely customizable. Within MMOG's participants may communicate with each other through a variety of means, including text chat or real time voice communication, using technologies such as VOIP to carry their messages.

Economic Crimes

Given the size of virtual world economies, it should not be surprising that many of the crimes committed in virtual spaces involve financial fraud or other nefarious activities for criminal economic gain. Virtual World economist Edward Castro nova has estimated the value of all the goods and services produced in virtual worlds to be between 7-12 billion US dollars per annum. He further noted the economic transfer of at least 1 billion dollars in virtual currencies per annum as of May 2009. As such, the virtual economy dwarfs the "real world" economy of dozens of countries around the world. The proliferation of virtual currencies, such as Linden Dollars, WoW gold, QQ coins and so many others, has created an attractive economic target for international organized crime groups. Long gone are the days where hackers engaged in criminal activities merely for the "fun" or "challenge" of the matter. Modern organized crime seeks first and foremost financial gain and the amount of money in MMORPG's poses an incredibly enticing target for them and the millions of MMORPG users can become to organized crime a readily accessible victim-base. The emergence of some dominant companies in the MMORPG field, such as Second Life and World of War craft, has meant that criminals can now create computer malware and social engineering scams to specifically locate and target large numbers of potential victims

Financial Frauds

There are several tried and tested ways of committing financial fraud in virtual worlds, including social engineering, exploiting or hacking MMORPG servers and the introduction of malicious computer code into an individual's virtual world environment. Social engineering attacks occur when cyber criminals enter an MMORPG or an associated, but independent, gaming forum where they search out users and offer them help or various bonuses to help "improve" their user experience or increase their gaming level. In exchange they solicit user names and passwords so that they can carry out the purported helpful work.

The Role of Malware

These malicious programs or computer Trojans enable a wide variety of criminal activities in MMORPG's, including the theft of virtual goods and money. The number of malware programs specifically directed at virtual worlds and online gaming has increased dramatically over the past few years. In fact, according to computer security company Kaspersky Laboratories, over 30,000 new malicious programs specifically targeting online games were introduced in 2008.

Money laundering

Over the past decade, a number of new alternative forms of payment have been introduced throughout the world to keep up the growing volume of electronic commerce. The most famous of these companies is PayPal, which became a wholly owned subsidiary of eBay in 2003. PayPal made it easier for payments to be made through the Internet and serves as an electronic alternative to traditional paper money, checks or bank money orders. It can be very useful for the vast majority of the planet's inhabitants that do have access to a credit card. Of course alternative payment systems also open up the doors to alternative forms of money laundering.

While PayPal was certainly revolutionary in its approach, it always settled transactions in well-established forms of national currency, such as dollars, yen or euros. Over the past few years however, a number of virtual worlds have begun to issue their own forms of currency. With names like the Linden Dollar (used by Linden Lab's Second Life), World of Warcraft Gold (from Blizzard Entertainment) or QQ Coins (by Tencent Limited), these virtual currencies are being used by literally tens of millions of people worldwide. There have been various estimates of the size of the virtual world economy, but some estimates have placed it in the billions of (US) dollars.

Given the vast sums of money being transferred among parties around the world, it should not be

surprising of course those criminals would want to take advantage of this money flow. With little if any regulation, virtual world economies are ripe for exploitation by organized crime, terrorists and others who wish to launder large sums of money.

While virtual world money laundering has theoretically been a possibility for some time, the following case clearly shows that theory has now been put into practice, to the tune of $38 million US dollars. As the Seoul Metropolitan Police Agency (SMPA) demonstrated, a group of Chinese and Korean criminals were able to successfully defraud Korean game players and then launder the funds through a number of business front companies back in mainland China.

Extortion

In further evidence demonstrating the growing value of virtual world goods, a court in China handed down a 3-year prison sentence in mid-2009 to a known gang member for extorting virtual goods. According to Chinese officials, three suspects cornered the victim in a cyber café and noticed he had a particularly large balance of virtual goods in his QQ-Tencent account. An assault ensued and the victim was forced to turn over the equivalent of nearly 100,000 RMB of the virtual currency QQ coins.(8) This case is interesting in that it shows that virtual goods must be of value in order for the arrest and prosecution to have occurred. As virtual goods proliferate, more and more individuals could become victims of virtual thefts and extortions.

Possession of Child Abuse Image

By the very nature of their entertainment value, virtual worlds and MMORPGs are attractive to people of all ages, and in particular to young people. The enticing cartoon-like graphics, the gaming potential and the entertainment value all make virtual worlds of interest to a younger audience. Of course this is not to say that children are the only ones using virtual worlds. In fact, across the board, most users in MMORPG's are in the 20's and 30's, but average ages vary greatly from game to game. Second Life tends to draw an older crowd than Disney's Club Penguin for example, which targets children from 6 to 14 years of age.

Many virtual worlds allow for outside connections and communications: text chats, real-time voice over internet protocol (VOIP) conversations, exchanges of photographic and video images with one another. While friends might want to do this for legitimate purposes, there certainly could be criminal implications as well.For example, a number of pedophiles could create avatars in Second Life providing false identification details. They could meet each other in various chat rooms/islands dedicated to "child love" or "Lolita" or any other such keyword and begin socializing with each other. One of the paedophiles (represented by his avatar) could readily build a movie theatre on the island of his choice and show whatever streaming video file he chooses. So in effect, it would be entirely possible to have a virtual room full of pedophiles watching real child abuse images (photos, videos, etc) of real children.

Age Play

While few would argue that the exchange of real child abuse images, whether done in person, on IRC (Internet-relay chat) or in a virtual world should be a criminal matter, the depiction of virtual children engaging in sexual activity proves much more difficult. For example, in Second Life, you can choose and dress you avatar as you wish, thus a 56 year old man could inhabit the avatar of a 12 year old girl and could then script that avatar to engage in various sexual activities. To those observing in Second Life, it would look as if the "12 year old girl" was engaging in sexual activities, while in reality it is the older man using the avatar for his own sexual purposes.

Should such activities be a crime? Across the world, government legislatures are answering this question differently. In Germany, Ireland and many other European countries the possession of

"virtual child pornography" is considered the legal equivalent of possessing "real" child pornography and is equally punishable by law. In the United States the courts have ruled that "virtual" child sex depictions are a form of fantasy and, as such, they do not constitute criminal behavior because no actual child was ever abused or photographed in the production of those virtual child abuse images. Others have argued that only somebody predisposed to abusing a real world child would want to act out sexually as a virtual child. Those in opposition responded that democratic societies should not have "thought police" and that a fantasy life that does not cross the threshold into harming others should not be criminalized.

One of the largest and most infamous cases of age play occurred in Second Life in an area known as "Wonderland." There, young "children" avatars were offering sex in a playground environment. The young children were in these context not real children, but graphical representations, the so-called avatars, and the playground was a virtual playground created with computer software. The case created a strong rebuke from law enforcement authorities and prosecutors in Germany opened a criminal case in the matter. Another such case was investigated by the British police.

Rape/Sexual Assault

Perhaps no other form of virtual world crime endangers quite as much passion amongst participants as the discussion of "virtual rape." To some, it is very much a crime as "real" world rape. Doubters dismiss the possibility outright, noting that rape is impossible without a human victim who has been physically attacked or violated. Despite the differences, more and more police agencies around the world are having victims of these types of crimes present themselves and demanding police redress. A "virtual rape" occurs when one person's avatar is forced into a sexual situation against his/her desire. To be clear, this type of crime is different from consenting adults acting out a fantasy version of rape for whatever reasons. Virtual world rape is alleged when one of the participants is an unwilling participant in the act. Graphics in MMORPG's and virtual worlds have progressed enormously, to the point that they can accurately represent real world scenarios fairly well. As such, an involuntary sexual assault could be perceived as having verisimilitude to the actual real world act. While many virtual worlds such as Second Life have built-in technical protections to prevent such activities from occurring, they can occur elsewhere through the introduction of malicious code that forces an avatar to do something against its will.

Again a review of the psychology of virtual worlds is critical here. To an individual who spends 12 hours a day inside a MMORPG living through their avatar, any activity that occurs to that avatar against its owner's will can be troubling. For some seeing one's avatar undergo a graphic representation of a violent sexual attack clearly would have a negative impact to the psyche of the avatar's owner. Whether this harm is as serious as a "real world rape" is very much debated openly and is beyond the scope of this report. That said, many such cases are occurring and are being reported to law enforcement around the world.

In Belgium recently, federal prosecutors asked the Belgian Federal Computer Crime Unit to travel to the scene of a crime in Second Life for the purpose of investigating a "virtual rape" involving a Belgian victim. This type of activity has been around for a very long period of time. The first most widely reported case of virtual rape was documented in 1993, long before today's MMORPG's existed. Despite how police may or may not feel about such cases, one thing is certain, they will be increasingly reported to police. As such, law enforcement should have a plan in place to deal with them and to secure any potential crime scene in search of evidence of criminal activity.

Stalking/Griefing

One of the most common complaints and potential criminal activities in virtual worlds/MMORPG is that of harassment, intimidation or stalking. This often occurs when an individual becomes the subject of unwanted attention or focus by another person (avatar) or group of them. In virtual worlds, this type of activity is commonly referred to as "grieving."

Perhaps it is not surprising that all the petty grievances, insults, arguments and disorders that occur in the "real world" also occur in "virtual world" spaces. A griever is not playing an online game or inhabiting an MMORPG for any useful purpose, except to harass or intimidate others. They may have uncovered undocumented technical aspects of the virtual world software and exploit these glitches or features to purely harass other players or inhabitants. For those victimized by such behavior, it can be extremely annoying and it could feel like the real world equivalent of stalking or harassment.

Prostitution

Prostitution is certainly common in virtual worlds and MMORPGs, but one must be careful about how one defines the term. Some individuals are willing to pay for their avatar to engage in simulated sexual conduct with another avatar for money (virtual currency or real). While this may or may not violate the terms of service of the virtual world itself, it would not be a criminal offense in many jurisdictions, assuming all parties were consenting adults. In other jurisdictions, even simulated sexual contact in exchange for money would be criminal.

While most police forces might not pursue strictly virtual prostitution between adults (especially when all activities were purely online within the MMORPG), there are many overlapping technologies that can make this type of activity a hybrid cross between the virtual and the real. For example, many virtual worlds allow users to incorporate VOIP communication into the MMORPG environment. Thus the addition of voice communication as part of the prostitution scenario might further push the boundaries of what is legal in some jurisdiction.

In other cases, pure acts of prostitution in the real world have taken on a virtual world component. In one of the most famous cases known as the "Epic Mount" case, a woman offered sexual encounters in the real world in exchange for money: 5,000 pieces of World of Warcraft gold. The woman claimed she needed the money to purchase her "epic flying mount." Since WoW gold can be exchange for real world currency (euros, dollars or yen) it has a real world value based on market conditions, and given the exchange of said currency for a real-world sexual act, that woman could be punishable in many jurisdictions.

Riots/Public Disorder

Though it might seem odd to talk about riots or public disorder issues in virtual worlds, they are in fact, not that uncommon. For example, during the most recent round of elections in Spain, most politicians had established a virtual presence in Second Life. Some politicians had even established their own avatars, which in turn campaigned, held rallies and put up election posters in virtual spaces. While things worked well for a while, politicians from one party were quickly overwhelmed with grieving by opposition supporters.

This is of course not the first time such a thing has happened. During a recent political rally by a far-right French politician, his posters were defaced, he had "exploding virtual pigs" hurled at him and Nazi swastikas were painted on campaign headquarters.

Surely when incidents as these occur, especially when they involve high-level politicians, law enforcement will be contacted. Whether or not police are able to respond to such matters under national law is another question. The fact is, however, that the public will increasingly expect their police service to handle incidents such as these.