Unit VI

CHAPTER 6

Confidentiality and Cyber Forensic

Syllabus

Introduction to Personally Identifiable Information (PII), Cyber Stalking, PII impact levels with examples Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law : Indian Perspective.

Syllabus Topic : Introduction to Personally Identifiable Information (PII)

6.1 Introduction to Personally Identifiable Information (PII)

6.1.1 Explain Personally Identifiable Information (PII). (Ref. Sec. 6.1)

Personally Identifiable Information (PII) is any data that could potentially recognize a specific individual. Any information that can be used to tell apart one person from another and can be used for deanonymizing anonymous data can be considered PII.

PII can be sensitive or non-sensitive. Non-sensitive PII is in order that can be transmitted in an unencrypted form without resulting in harm to the individual.

Non-sensitive PII can be simply gathered from public records, phone books, corporate directories and websites.

Sensitive PII is in turn which, when disclosed, could result in harm to the individual whose privacy has been breached.

Sensitive PII should therefore be encrypted in transfer and when data is at rest. Such information adds biometric information, medical information, in Person Identifiable Financial Information (PIFI) and unique identifiers such as passport or Social Security numbers.

Syllabus Topic : Cyber Stalking

6.2 Cyber Stalking

Q. 6.2.1 What is Cyber stalking? Explain with example. (Ref. Sec. 6.2)

- Cyber stalking is a crime in which the attacker harasses a victim using electronic message, such as e-mail or Instant Messaging (IM), or messages posted to a Web site or a discussion group.
- A cyber stalker relies upon the secrecy afforded by the Internet to allow them to stalk their victim without being detected.
- Cyber stalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with merely annoying messages.
- WHOA (Working to Halt Online Abuse), an online organization committed to the cyber stalking problem, reported that in 2001 58% of cyber stalkers were male and 32% female (presumably in some cases the perpetrator's gender is unknown). In a difference known as corporate cyber stalking, an organization stalks an individual.
- Corporate cyber stalking (which is not the same thing as corporate monitoring of e-mail) is usually initiated by a high-ranking company official with a grudge, but

may be conducted by any number of employees within the organization. Less frequently, corporate cyber stalking involves an individual pestering a corporation.

- WHOA reported that, in 2001, cyber stalking began with e-mail messages most frequently, followed by message boards and forums messages, and less frequently with chat. In some cases, cyber stalking develops from a real-world stalking incident and continues over the Internet.
- However, cyber stalking is also sometimes followed by stalking in the physical world, with all its assistant dangers. According to former U.S. Attorney General Janet Reno, cyber stalking is often "a prologue to more serious behaviour, including physical violence".
- In 1999, a New Hampshire woman was murdered by the cyber stalker who had endangered her in e-mail messages and posted on his Web site that he would kill her.
- There are a number of effortless ways to guard against cyber stalking. One of the most useful protection is to stay anonymous yourself, rather than having an identifiable online presence: Use your primary e-mail account only for communicating with people you trust and arrangement an anonymous e-mail account, such as Yahoo or Hotmail, to use for all your other communications.
- Set your e-mail program's filtering options to avert delivery of unwanted messages. When choosing an online name, make it different from your name and gender-neutral. Don't put any identifying particulars in online profiles.
- Should you become the victim of a cyber stalker? The most effective course of action is to report the criminal to their Internet service provider (ISP). Should that option be impossible, or unproductive? The best thing is to change your own ISP and all your online names.
- WHOA news that over 80% of cases reported in 2001 and 2002 were resolved by these methods, while 17% were reported to law enforcement officials.
- Cyber stalking, cyber squatting, and cyber terrorism are among the rising number of new computer and internet-related crimes, sometimes referred to collectively as cybercrime.

Syllabus Topic : PII Impact Levels with Examples Cyber Stalking

6.3 PII Impact Levels with Examples Cyber Stalking

Q. 6.3.1 Explain different impact levels of PII with an example. (Ref. Sec. 6.3)

Q. 6.3.2 Distinguish Cyber stalking from other acts. (Ref. Sec. 6.3)

- With the virtual world becoming part of the social lives of adults and minors alike, new attack vectors emerged to increase the severity of human-related attacks to a level the community have not experience before. This article finds out, shares and summarize on how technology could emerge further to counteract and mitigate the damage caused by online perpetrators.
- The review encourages approaching online harassment, nuisance, bullying, grooming and their likes with an Incident Response methodology in mind. This includes a detection phase utilizing automated methods to recognize and classify such attacks, conduct digital forensic investigations to analyse the nature of the offence and reserve evidence, taking preventive measures as part of the reaction towards the problem such as filtering unwanted communications and finally looking at how we can rely on applicable computing to support and educate thevictims.
- **Cyber stalking** is the use of the Internet or other electronic means to stalk or harass a person, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.
- Cyber stalking is often accompanied by real time or offline stalking. In many areas, such as California, both

are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

A stalker may be an online stranger or a person whom the person knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

- Cyber stalking is a crime regarded in the US and many other judicial systems as more serious than a misdemeanourunder various state anti-stalking, slander and harassment laws.
- A conviction can result in a restraining order, probation, or criminal penalties against the attacker, including jail.
- There have been a number of attempts by experts and legislators to define cyber stalking. It is generally understood to be the use of the Internet or other electronic means to stalk or harass a person, a group, or an organization.
- Cyber stalking is a form of cyber bullying. The terms are frequently used interchangeably in the media. Both may include false accusations, defamation, slander and libel.
- Cyber stalking may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Cyber stalking is frequently accompanied by real-time or offline stalking. Both forms of stalking may be criminal offenses.
- Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself.
- Technology ethics professor Lambèr Royakkers defines cyber stalking as perpetrated by someone without a current relationship with the victim. About the abusive effects of cyber stalking, he writes that, it is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together.

Distinguishing cyber stalking from other acts

- It is important to draw a distinction between cyber-trolling and cyber-stalking.
- Research has shown that actions that can be supposed to be harmless as a one-off can be considered to be trolling, whereas if it is part of a persistent campaign then it can be considered stalking.

Sr. No.	Motive	Mode	Gravity	Description
1	Playtime	Cyber-bantering	Cyber-trolling	In the moment and quickly regret
2	Tactical	Cyber-trickery	Cyber-trolling	In the moment but don't regret and continue
3	Strategic	Cyber-bullying	Cyber-stalking	Go out of way to cause problems, but without a sustained and planned long-term campaign
4	Domination	Cyber-hickery	Cyber-stalking	Goes out of the way to create rich media to target one or more specific individuals.

- Cyber stalking author Alexis Moore separates cyber stalking from identity theft, which is economically motivated. Her definition, which was also used by the Republic of the Philippines in their legal description, is as follows : "Cyber stalking is a technologically-based

attack on one person who has been targeted particularly for that attack for reasons of anger, revenge or control".

- Cyber stalking can take many forms including :
  1. Harassment, embarrassment and humiliation of the victim
  2. Emptying bank accounts or other economic control such as defilement of the victim's credit score
  3. Harassing family, friends and employers to segregate the victim
  4. Scare tactics to instill fear and more.

Identification and detection

Q. 6.3.3 How one can identify and detect Cyber stalking? (Ref. Sec. 6.3)

Q. 6.3.4 List out the key factors in identifying Cyber stalking. (Ref. Sec. 6.3)

- Cyber Angels has written about how to identify cyber stalking :

  When identifying cyber stalking "in the field," and mostly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation : malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment and threats.

- A number of key factors have been identified in cyber stalking :
  - **False accusations :** Many cyber stalkers try to harm the reputation of their victim and turn other people against them. They post fake information about them on websites. They may set up their own websites, blogs or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions such as Wikipedia or Amazon.com.
  - **Attempts to gather information about the victim :** Cyber stalkers may advance to their victim's friends, family and work colleagues to obtain personal information. They may publicize information on the Internet, or hire a private detective.
  - Monitoring their target's online activities and attempting to trace their IP address in an attempt to gather more information about their victims.
  - **Encouraging others to annoy the victim :** Many cyber stalkers try to involve third parties in the annoyment. They may say the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
  - **False victimization :** The cyber stalker will claim that the victim is annoying him or her. Bocij writes that this fact has been noted in a number of well-known cases.
  - **Attacks on data and equipment :** They may try to harm the victim's computer by sending viruses.
  - **Ordering goods and services :** They order items or subscribe to magazines in the victim's name.
- These frequently involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.
- **Arranging to meet :** Young people face a particularly high risk of having cyber stalkers try to set up meetings between them.
- The posting of defamatory or derogatory statements: Using web pages and message boards to incite some response or reaction from their victim.

Prevalence and Impact

Q. 6.3.5 Write a short note on : Prevalence and impact. (Ref. Sec. 6.3)

- According to Law Enforcement Technology, cyber stalking has increased exponentially with the expansion of new technology and new ways to stalk victims.

Disgruntled employees pose as their bosses to post open messages on social network sites, spouses use GPS to track their mates' every move.

Even police and prosecutors find themselves at risk, as gang members and other organized criminals come across where they live - frequently to intimidate them into dropping a case.

In January 2009, the Bureau of Justice Statistics in the United States released the study "Stalking Victimization in the United States", which was sponsored by the Office on Violence Against Women.

The report, based on supplemental data from the National Crime Victimization Survey, showed that one in four stalking sufferers had been cyber stalked as well, with the perpetrators using internet-based services such as email, instant messaging, GPS, or spyware.

The final report stated that around 1.2 million victims had stalkers who used technology to find them.

The Rape, Abuse and Incest National Network (RAINN), in Washington D.C. has released statistics that there are 3.4 million stalking sufferer each year in the United States. Of those, one in four reported experiencing cyber stalking.

According to Robin M. Kowalski, a social psychologist at Clemson University, cyber bullying has been shown to cause higher levels of anxiety and depression for sufferer than normal bullying.

Kowalksi states that much of this stems from the anonymity of the perpetrators, which is a common feature of cyber stalking as well. According to a study by Kowalksi, of 3,700 bullied middle-school students, a quarter had been subjected to a form of annoyment online.

Types

6.3.6 Enlist the different types of Cyber stalker attacks. (Ref. Sec. 6.3)

1. Stalking by strangers

- According to Joey Rushing, a District Attorney of Franklin County, Alabama, there isn't a lone definition of a cyber stalker - they can be either strangers to the prey or have a former/present relationship.
- "Cyber stalkers come in all shapes, sizes, ages and backgrounds. They tour Web sites looking for an opportunity to take advantage of people".

2. Gender-based stalking

- Annoyment and stalking because of gender online is common, and can include rape threats and other threats of violence, as well as the posting of the sufferer's personal information.
- It is blamed for limiting sufferer activities online or driving them offline entirely, thereby impeding their participation in online life and undermining their autonomy, dignity, identity, and opportunities.

3. Of intimate partners

- Cyber stalking of intimate partners is the online annoyment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency.
- Annoyers may send repeated insulting or threatening e-mails to their sufferer, monitor or disrupt their sufferer' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim does not want. They may also use the Internet to research and compile personal information about the victim, to use in order to annoy him or her.

4. Of celebrities and public persons

- Profiling of stalkers shows that about always they stalk someone they know or, via delusion, think they know, as is the case with stalkers of celebrities or public persons in which the stalkers feel they know the celebrity yet the celebrity does not know them. As part of the risk they take for being in the public eye,

1. Hacking

- It is an unlawful practice by which a hacker breaches the computer's security system of someone for personal interest.

2. Unwarranted mass-surveillance

- Mass surveillance means surveillance of a considerable fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

3. Child pornography

- It is one of the most atrocious crimes that is brazenly practiced across the world.
- Children are sexually abused and videos are being made and uploaded on the Internet.

4. Child grooming

- It is the practice of establishing an emotional connection with a child mainly for the purpose of child-trafficking and child prostitution.

5. Copyright infringement

- If someone infringes someone's protected exclusive rights without permission and publishes that with his own name, is known as copyright infringement.

6. Money laundering

- Unlawful possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legal business.
- In added words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

7. Cyber-extortion

- When a hacker hacks someone's email server, or computer system and load money to reinstate the system, it is known as cyber-extortion.

8. Cyber-terrorism

- Normally, when someone hacks government's security system or intimidates government or such a big organization to move forward his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Syllabus Topic : PII Confidentiality Safeguards

6.5 PII Confidentiality Safeguards

Q. 6.5.1 Discuss PII confidentiality safeguards. (Ref. Sec. 6.5)

- Personally identifiable information (PII) is any information that can be used to recognize, contact, or locate an individual, either alone or combined with other easily accessible sources.
- It includes information that is connected or linkable to an individual, such as medical, educational, financial and employment information.
- Examples of data elements that can identify an individual contain name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number.
- Safeguarding university-held PII (and other sensitive information) is the accountability of each and every member of the University's workforce. Regardless of your role, you should know what PII is and your accountability in ensuring its protection.
- Although society has always relied on personal identifiers, essential and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information.
- The protection of PII and the on the whole privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations spoiled

should such PII be inappropriately accessed, used, or disclosed. Examples of laws related to different types of PII are listed below :

- HIPAA/HITECH - Health related information.
- GLBA - Financial information.
- Privacy Act - Fair Information Practices for PII held by Federal Agencies.
- COPPA - Protects children's privacy by allowing parents to control what information is collected.
- FERPA - Student's personal information.
- FCRA - Collection and use of consumer information.

- Such laws attempt to restrict corporations from incorrectly sharing PII and impose requirements for appropriately protecting such information.
- Legally collecting and selling PII has become lucrative, but PII can also be exploited by criminals to steal a person's identity or commit other crimes.
- According to FBI statistics, identity theft continues to be one of the nation's fastest growing crimes and can cause both financial and emotional damage to its sufferer. Due to this threat, many governments have enacted legislation to bound the distribution of personal information.
- The following list contains examples of information that may be considered PII.
  - Name, such as full name, maiden name, mother's maiden name, or alias
  - Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
  - Address information, such as street address or email address
  - Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
  - Telephone numbers, including mobile, business, and personal numbers
  - Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
  - Information identifying personally owned property, such as vehicle registration number or title number and related information
  - Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

Syllabus Topic : Information Protection Law - Indian Perspective

6.6 Information Protection Law : Indian Perspective

Q. 6.6.1 Explain Information protection law : Indian perspective. (Ref. Sec. 6.6)

Q. 6.6.2 What are different types of attacks by Hackers? (Ref. Sec. 6.6)

Q. 6.6.3 Explain the terms :
(i) Virus (ii) Phishing
(iii) Spoofing (iv) Phone phishing
(v) Internet pharming (Ref. Sec. 6.6)

What Is Cyber Crime?

- Cyber terrorists typically use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information.
- Internet is one of the way by which the offenders can gain such price sensitive information of companies,

firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling unlawful articles, pornography etc.

- This is done through many methods such as phishing, spoofing, pharming, internet phishing, wire transfer etc. and use it to their own advantage without the permission of the individual.
- Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and endangered by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages.
- And its been reported that many institutions in US, Britain and Europe have furtively paid them to prevent huge meltdown or collapse of confidence among their consumers.

Emergence of Information Technology Act, 2000

- In India, the Information Technology Act 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
- This was the first step towards the Law involving to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. It was enacted taking into thought UNICITRAL model of Law on e-commerce 1996.
- Some notable Provisions Under The Information Technology Act, 2000.
  - Sec. 43 : Damage to Computer system etc.
  - Sec. 66 : Hacking (with objective or knowledge) Compensation for Rupees 1crore. Fine of 2 lakh rupees, and captivity for 3 years.
  - Sec. 67 : Publication of obscene material in e-form Fine of 1 lakh rupees, and captivity of 5years, and double conviction on second offence.
  - Sec. 68 : Not complying with directions of controller
  - Sec. 70 : Attempting or securing access to computer.
  - Sec. 72 : For breaking confidentiality of the information of computer
  - Sec. 73 : Publishing false digital signatures, false in certain particulars
  - Sec. 74 : Publication of Digital Signatures for fraudulent purpose Fine upto 2 lakh and imprisonment of 3 years.
- Captivity upto 10 years. Fine upto 1 lakh and imprisonment upto 2 years Fine of 1 lakh, or imprisonment of 2 years or both. Captivity for the term of 2 years and fine for 1 lakh rupees.

Types of Attacks By Hackers

- Hacker is computer expert who uses his knowledge to get unauthorized access to the computer network. He is not any person who intends to break through the system but also includes one who has no intention todamage the system but intends to learn more by using ones computer.
- Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider or an employee is pretty prominent in present date. Section 66(b) of the Information Technology Act 2000, provides punishment of imprisonment for the period of 3 years and fine which may extent to two lakhs rupees,or with both.
- Banks and other financial institutions are threatened by the terrorist groups to use their sensitive information resulting in deep loss and in turn ask for ransom amount from them. There are various methods used by hackers to gain unauthorised access to the computers distant from use of viruses like Trojans and worms etc.

Therefore if anyone secures access to any computer without the permission of the owner shall be likely to pay damages of 1 crore rupees under Information Technology Act, 2000.

Computer system here means a device including input and output support devices and systems which are capable of performing logical, arithmetical, data storage and reclamation, communication control and other functions but excludes calculators.

Unauthorised access under Section 43 of the Information Technology Act 2000 is punishable regardless of the intention or purpose for which unauthorised access to the computer system was made. Owner needn't prove the facto of loss, but the fact of it been used without his authorisation.

- Case of **United States v. Rice** would be important in this consider where defendant on the request of his friend (who was been beneath investigation by IRS officer) tried to find the status of his friends case by using officers computer without his approval.
- Though it didn't cause any spoil/loss to the plaintiff (officer) but was convicted by the Jury for accessing the computer system of a Government without his authority and his sincerity was later on confirmed. Even if one provides any help to the other to gain any unauthorised access to the computer he shall be liable to pay damages by way of compensation of Rupees 1 crore.
- Does turning on the computer leads to unauthorized access? The mensrea under section 1 of the Computer misuse Act, 1990 comprises of two elements there must be an intent to secure an access to any programme or data held in any computer, and the person must know that he intends to secure an unauthorized access.
- Though section 1 (1) (a) requires that second computer must be involved but the judiciary in the case of R v. Sean Cropp, believed that the Parliament would have intended to limit the offence even if single computer system was involved.

(A) Computer Viruses

- Viruses are used by Hackers to contaminate the user's computer and dent data saved on the computer by use of payload in viruses which carries damaging code.
- Person would be liable under I.T Act only when the consent of the owner is not taken before inserting virus in his system.
- The contradiction here is that though definite viruses causes temporary interruption by showing messages on the screen of the user but still its not punishable under Information Technology Act 2000 as it doesn't cause tangible damage.
- But, it must be made punishable as it would plunge under the ambit of unauthorised access though doesn't cause any damage.
- Harmless viruses would also plunge under the expression used in the provision to unsurp the normal operation of the computer, system or network. This ambiguity needs reconsideration.

(B) Phishing

- By using e-mail messages which entirely resembles the original mail messages of customers, hackers can ask for verification of certain information, like account numbers or passwords etc.
- Here customer might not have knowledge that the e-mail messages are unreliable and would fail to identify the originality of the messages.This results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it.

(C) Spoofing

- This is carried on by use of unreliable Websites or e-mails.
- These sources copy the original websites so well by use of logos, names, graphics and even the code of real banks site.

(D) Phone Phishing

- Is done by use of in-voice messages by the hackers where the customers are asked to disclose their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc.

(E) Internet Pharming

- Hacker here aims at redirecting the website used by the customer to another fake website by hijacking the sufferer DNS server (they are computers responsible for resolving internet names into real addresses - signposts of internet), and changing his I.P address to fake website by manipulating DNS server. This redirects user's original website to a false deceptive website to gain unauthorised information.

(F) Risk Posed On Banks and Other Institutions

- Wire transfer is the means of transferring money from one account another or transferring cash at cash office. This is most convenient way of transfer of cash by customers and money laundering by cyber terrorists.
- There are many guidelines issued by Reserve Bank of India (RBI) in this view, one of which is KYC (Know Your Customer) norms of 2002. Main objective of which is to :
  1) Ensure appropriate customer identification, and
  2) Monitor the transaction of suspicious nature and report it to appropriate authority every day bases.

(G) Publishing Pornographic Material in Electronic Form

- Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and broadcast of any material in electronic that lascivious or appeals to the prurient interest a crime, and punishable with captivity which may extend to 5 years and fine of 1 lakh rupees and subsequent offence with an captivity extending to 10 years and fine of 2 lakhs.
- Various tests were laid down slowly in course of time to determine the actual crime in case of obscene material published in electronic form on net.
- Hicklin test was adopted in America in the case of Regina v. Hicklin wherein it was seized that if the material has tendency is to deprive and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.
- In Indian situation the case of Ranjeet D. Udeshi v. State of Maharashtra the Supreme Court admitted that Indian Penal Code doesn't term obscenity though it provides punishment for publication of obscene matter.
- There are very thin line existing between a material which could be called obscene and the one which is artistic.
- Court even strained on need to maintain balance between fundamental right of freedom of speech and expression and public decency and morality. If matter is likely to degrade and corrupt those minds which are open to influence to whim the material is likely to fall. Where both obscenity and artistic matter is so mixed up that obscenity falls into shadow as its insignificant then obscenity may be overlooked.
- In the case of Miller v. California it was held that local community standard must be applied at the time of determination of the offence.
- As it can traverse in many jurisdictions and can be accessed in any part of the globe. So wherever the material can be accessed the community standards of that country would be applicable to determine the offence of publication of obscene material posted in electronic form. Though knowledge of obscenity under Information Technology Act 2000 and Indian Penal Code may be taken as justifying factor but doesn't take the case out of the provision.
- Section 72 of Information Technology Act, 2000 provides punishment for an unauthorised access or, exposé of that information to third person punishable with an captivity upto 2 years or fine which may extend to 1 lakh rupees or with both.

- English courts have also dealt with an issue as to what activities would form crime under existing legislation, in the case of R. v. Fellows and Arnold it was held that the legislation before the 1994 amendment would also facilitate computer data to be considered a copy of an indecent photograph and making images available for downloading from the website would constitute material being distributed or shown.
- Statute is wide enough to deal with the use of computer technology.

(H) Investment Newsletter

- We usually get newsletter providing us free information recommending that investment in which field would be lucrative.
- These may sometimes be a fraud and may origin us huge loss if relied upon.
- False information can be spread by this method about any company and can cause massive inconvenience or loss through junk mails online.

(I) Credit Card Fraud

- Huge loss may reason to the victim due to this kind of fraud. This is done by publishing false digital signatures.
- Most of the people misplace credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.

Measures to Curb the Crime

- Though by course of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers, crackers etc.
- Various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users.

Few basic major measures used to curb cyber crimes are as follows :

(A) Encryption

- This is considered as an important tool for shielding data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way excluding for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.
- Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method.
- Usual problem lies during the allocation of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill.
- Public key encryptography was one solution to this where the public key could be known to the whole world but the private key was only identified to receiver. It's very difficult to derive private key from public key.

(B) Synchronized Passwords

- These passwords are schemes used to change the password at users and host token. The password on synchronized card changes every 30-60 seconds which only makes it legitimate for one time log-on session.
- Other functional methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases.

(C) Firewalls

- It creates wall between the system and possible intruders to protect the confidential documents from being leaked or accessed.
- It would only let the data to flow in computer which is known and verified by ones system. It only permits access to the system to ones already registered with the computer.

(D) Digital Signature

- Are created by using means of cryptography by applying algorithms.
- This has its important use in the business of banking where customers signature is identified by using this method before banks enter into huge transactions.

Investigations and Search Procedures

- Section 75 of Information Technology Act, 2000 takes care of jurisdictional part of cyber crimes, and one would be punished irrespective of his nationality and place of commission of offence.
- Power of inquiry is been given to police officer not below the rank of Deputy Superintendent of police or any officer of the Central Government or a State Government authorised by Central Government.
- He may enter any public place, conduct a search and arrest without warrant person who is reasonably expected to have committed an offence or about to commit computer related crime.
- Accused has to be shaped before magistrate within 24 hours of arrest. Provisions of Criminal Procedure Code, 1973 regulate the procedure of entry, search and arrest of the accused.

6.7 Problems Underlying Tracking of Offence

Q. 6.7.1 What are the challenges the system face to track the offence ? (Ref. Sec. 6.7)

- Most of the times the offenders commend crime and their identity is hard to be identified. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of additional countries.
- Most of the countries not have skilled law enforcement personnel to deal with computer and even broader Information technology related crimes.
- Usually law enforcement agencies also don't take crimes serious, they have no significance of enforcement of cyber crimes, and even if they undertake to investigate they are posed with limitation of extra-territorial nature of crimes.

How Efficient Is Information Technology Act 2000 ?

- It can't be disputed that Information Technology Act, 2000 though provides definite kinds of protections but doesn't cover all the spheres of the I.T where the protection must be provided.
- Copyright and trade mark violations do occur on the net but Copy Right Act 1976, or Trade Mark Act 1994 are quiet on that which specifically deals with the issue. Therefore have no enforcement machinery to ensure the protection of domain names on net.
- Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn't hinder the violations caused in the cyberspace.
- Even the Internet Service Providers (ISP) who provides some third party information without human intervention is not made liable under the Information Technology Act, 2000.
- One can easily take cover under the exemption clause, if he proves that it was committed without his knowledge or he exercised due diligence to avert the offence. Its hard to prove the commission of offence as the terms due diligence and lack of knowledge have not been clear anywhere in the Act.
- And unfortunately the Act doesn't mention how the extra territoriality would be imposed. This aspect is completely ignored by the Act, where it had come into existence to look into cyber crime which is on the face of it an international problem with no territorial boundaries.

Data Protection

- Information stored on the owner of the computer would be his property and must be protected there are many ways such information can be misrepresented by ways like unauthorized access, computer viruses, data typing, modification erasures etc.
- Legislators had been continuously confronted with problem in balancing the right of the individuals on the computer information and other peoples claim to be allowed access to information under Human Rights.
- The first enactment in this regard was Data Protection Act by Germany in the year 1970. This was widely received by the world and also contributed to the Information Technology Act.
- The origin of laws on date protection dates back to 1972 when United Kingdom created a committee on privacy which came up with ten principles, on the bases of which data protection committee was set up.
- Data Protection Act, 1984 (DPA) was United Kingdoms response to the Council of Europe Convention 1981, this Act lacked proper enforcement mechanism and has done little to enforce individuals rights and freedoms.
- European Union directive in 1995, European Convention of Human Rights (ECHR), Human Rights Acts, and further introduction of Data Protection Act, 1998 have done a large amount in the field of Data protection in today's date.
- Data Protection Act has following aims and objectives: Personal information shall only be obtained for lawful purpose, it shall only be used for that purpose, mustnot be disclosed or used to effectuate any unlawful activity, and must be disposed off when the purpose is satisfied.
- Though Data Protection Act aims at protecting privacy issues related to the information but still we find no reveal of the word privacy in the Act, nor is it defined, further the protection comes with various exemptions, including compulsory notification from the Commissioner in certain cases of the personal data.
- Due to the change in the regime of information technology for the date European Convention came, on which the Act is based changes in the Act is advised for matching the present situation and curbing the crime in efficient way.
- There is no Data Protection Act in India, the only provisions which talks about data protection are Section 72 and Section 43 of Information Technology Act, 2000.
- There must be a new Law to deal with the situation for a person to know that the checker is processing his data concerning him and also that he must know the purpose for which it has been processed.
- It is a fundamental right of the Individual to hold private information concerning him provided under Article 21 of the Indian Constitution, which says: No person shall be rundown of his life or personal liberty except according to procedure established by law.
- And due to the increasing trend of the Crime rate in the field separate legislation is required in this environment for better protection of individuals.

Chapter Ends...

❑❑❑