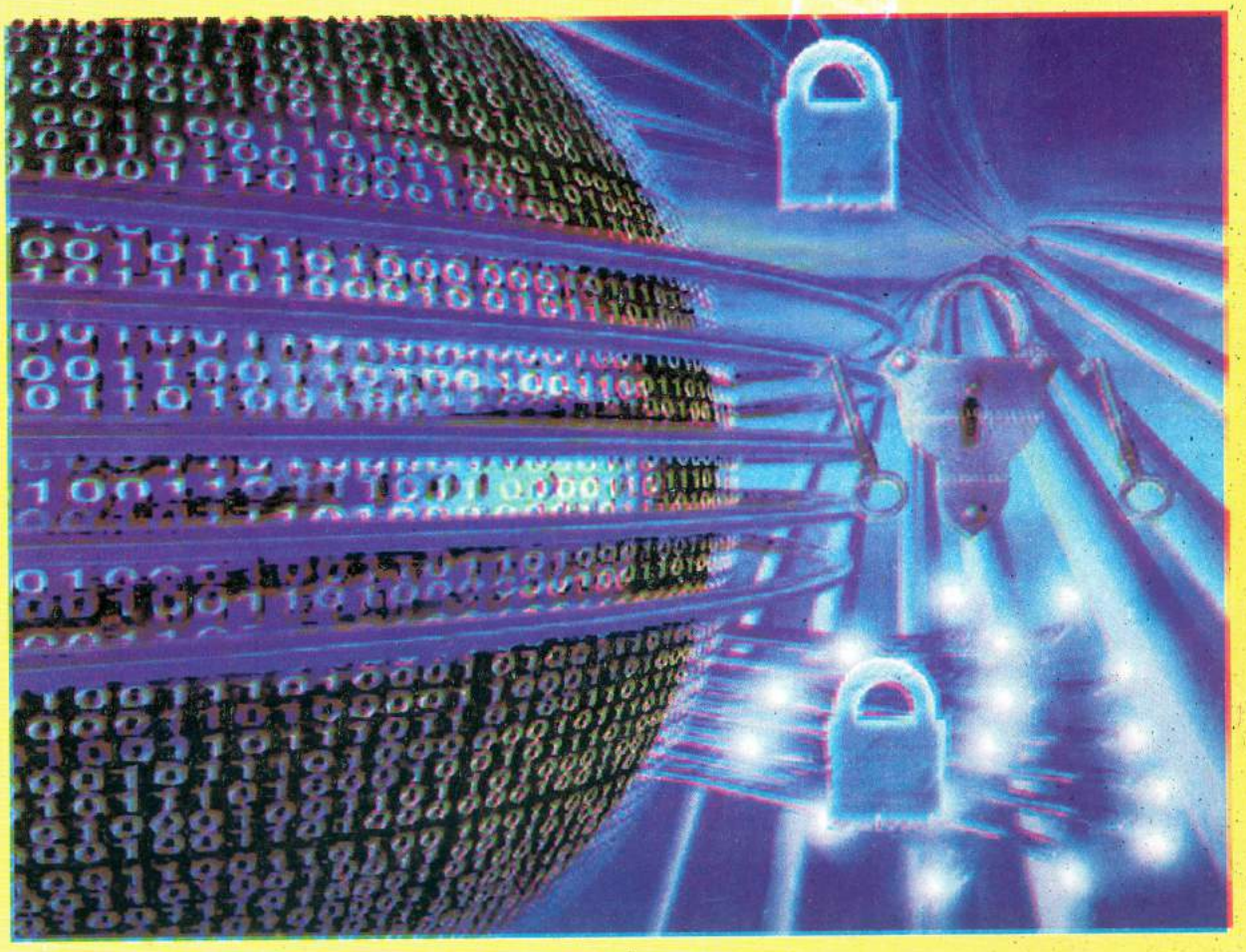
ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSE-024
Policy, Standards and Laws



Cyber Crimes and Regulation

4

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्रा की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

- इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

- Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSE-024
Policy, Standards and Laws

Block

4

CYBER CRIMES AND REGULATION

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writer

Adv. Pavan Duggal
Supreme Court of India
and President Cyberlaws.Net
(Unit 1, 2, 3 & 4)

Block Editors

Adv. Vaishali Kant
B.A.LL.B, LLM
National Law School of India University, Bangalore

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training
IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School Vocational Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

August, 2011

ISBN : 978-81-266-5725-4

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed At :- Print Pack (India),215/21,Ambadker Gali Moujpur Delhi - 53 .

BLOCK INTRODUCTION

Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Additionally, although the terms computer crime and cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important and should be properly regulated. This block comprises of four units and is designed in the following way;

The **Unit one** deals with Computer crime, or cyber crime which refers, to criminal exploitation of the Internet. Computer crime includes traditional criminal acts committed with a computer, as well as new offenses that lack any parallels with non-computer crimes. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. Cyber crimes mainly divided into breaches of physical security, personnel security, communications and data security and operation security

The **Unit two** deals with the conventional crimes happened through computer. It is essential to know the relation of conventional crimes with the cyber crimes. Although such crimes are required to be controlled and prevented in order to have proper utilization of cyber space in the growth and development work

The **Unit three** deals with the tort involved in the cyberspace or committed on a computer network. Torts or Civil wrongs are wrongs committed against private entities such as companies or private citizens, but are not necessarily offences

tort committed in cyberspace. Cyber crimes are
ıter database and systems. They usually use the
for their unlawful act either to gain information
mage to the owner of that intangible sensitive

iiscussion or
the possibility of data alteration and
ıe and database. This unit discusses the ways or
d the ways for preventing the same.

k.

urely for educational purposes. Every effort has
ght holders of material reproduced in this book.
ccurred, the publishers and editors apologize and
essary corrections in future editions of this book.

UNIT 1 INTRODUCTION TO COMPUTER CRIMES

Structure

1.0 INTRODUCTION

With the advent of the computer, criminals have found a new way to commit crimes. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. A computer crime is any unlawful activity that is done using a computer. This definition can extend to traditional crimes that use a computer, such as counterfeiting money. It also includes more tech-savvy crimes, such as phishing or logic bombs. Using a computer in this way, a criminal may be able to conduct unlawful activity with more anonymity and may be able to get away with more before he is caught.

1.1 OBJECTIVES

After going through this Unit, you should be able to:

- explain and define computer crime;
- understand kinds of computer crimes;
- understand the types of breaches of communications and data security and operation security; and
- explain case study in cyber crimes.

1.2 WHAT IS A COMPUTER CRIME?

Computer crime or cybercrime, refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography

and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as espionage, financial theft and other cross-border crimes sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat[1].

Computer crime includes traditional criminal acts committed with a computer, as well as new offenses that lack any parallels with non-computer crimes. The diversity of offenses renders any narrow definition unworkable. The U.S. Department of Justice (DOJ) broadly defines computer crimes as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution." Accurate statistics on the extent of this phenomenon have proven to be elusive because of the difficulty in adequately defining computer crimes[2].

Stalking, soliciting sex and counterfeiting can all be considered a type of computer crime if a computer is used to commit them. These crimes are unique because they can be done with or without a computer. They are not, however, considered computer crimes unless a computer is used in the process of committing them. For example, it would be considered a computer crime if a criminal uses a graphic design program to counterfeit money. Likewise, a person who cyber stalks another by using a computer to harass them also is committing a computer crime[3].

Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet[4].

1.2.1 New Crimes in Cyberspace[5]

There are three major classes of criminal activity with computers: (i) unauthorized use of a computer, which might involve stealing a username and password or might involve accessing the victim's computer via the Internet through a backdoor operated by a Trojan horse program, (ii) Creating or releasing a malicious computer program (e.g. computer virus, worm, Trojan Horse), (iii) harassment and stalking in cyberspace.

1.2.2 Old Crimes

When lay people hear the words "computer crime", they often think of obscene pictures available on the Internet or solicitation of children for sex by pedophiles via chat rooms on the Internet. The legal problem of obscenity on the Internet is mostly the same as the legal problem of obscenity in books and magazines, except for some technical issues of personal jurisdiction on the Internet.

Similarly, many crimes involving computers are no different from crimes without computers: the computer is only a tool that a criminal uses to commit a crime. For example, using a computer, a scanner, graphics software and a high-quality color laser or ink jet printer for forgery or counterfeiting is the same crime as using a old-fashioned printing press with ink.

---

[1] http://en.wikipedia.org/wiki/Computer_crime
[2] http://ecommerce.hostip.info/pages/237/Computer-Crime-DEFINITIONS.html
[3] http://www.wisegeek.com/what-is-a-computer-crime.htm
[4] http://www.webopedia.com/TERM/C/cyber_crime.html
[5] http://www.rbs2.com/ccrime.htm

Stealing a laptop computer with proprietary information stored on the hard disk inside the computer is the same crime as stealing a briefcase that contains papers with proprietary information.

Using the Internet or online services to solicit sex is similar to other forms of solicitation of sex and so is not a new crime.

Using computers can be another way to commit either larceny or fraud.

False origin

There are many instances of messages sent in the name of someone who neither wrote the content nor authorized the sending of the message. For example: E-mails with bogus from: addresses were sent automatically by malicious programs (e.g. the Melissa virus in 1999, the BadTrans worm in 2001, the Klez program in 2002).

Posting messages in an Internet newsgroup or online bulletin board with a false author's name that is intended to harm the reputation of the real person of that name.

Similar issues arise in both: (1) fictitious From: addresses in some unsolicited commercial e-mail, also called spam or junk e-mail and (2) fictitious source IP addresses in denial of service attacks.

Online activities are just as vulnerable to crime and can compromise personal safety just as effectively as common everyday crimes. Lawmakers, law enforcement and individuals need to know how to protect themselves and the persons for which they are responsible. Crimes have existed long before computers and the internet were made available to the general public. The only difference involves the tools used to commit the crime[6].

Cyber crimes refer to all crimes performed or resorted to by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system[7].

Computer Crime is any crime where

- Computer is a target.
- Computer is a tool of crime
- Computer is incidental to crime

1.3 DEFINITION OF A COMPUTER CRIME

A computer crime is any illegal action where the data on a computer is accessed without permission. This access doesn't have to result in loss of data or even data modifications. Arguably the worst computer crime occurs when there are no indications that data was accessed.

Computer crime is often attributed to rogue hackers and crackers, but increasingly organized crime groups have realized the relative ease of stealing data with relative low-level of risk. Government organizations are also rumoured to be involved with hacking in to computer systems, but the legality of such actions is far too grey an area to be discussed here[8].

---

[6] http://www.brighthub.com/internet/security-privacy/articles/3435.aspx

[7] http:/www.cybercellmumbai.com/files/Types%20of%20cyber%20crime.pdf

[8] http://www.mariosalexandrou.com/definition/computer-crime.asp

Computer crime[9] or e-crime is crime in which a computer plays an essential part.

Exactly what is illegal varies greatly from territory to territory. Consequently, the growth of international data communications and in particular the Internet has made these crimes both more common and more difficult to police.

Examples of computer crime are:

- Fraud achieved by the manipulation of computer records.
- Spamming where this is outlawed completely or where regulations controlling it are violated.
- Deliberate circumvention of computer security systems.
- Unauthorised access to or modification of programs data.
- Industrial espionage by means of access to or theft of computer materials.
- Identity theft where this is accomplished by use of fraudulent computer transactions.
- Writing or spreading computer viruses or worms.
- Salami slicing is the practice of stealing money repeatedly in extremely small quantities
- The use of a computer to take or alter data or to gain unlawful use of computers or services[10].

Cybercrime is further described as crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. [Thesaurus dictionary]

Computer crime refers to crimes against a computer through acts that attack a computer system. [The Fight Against Computer Crime by Racheal Phillips]

[11]**Cybercrime** is also known as computer crime. Any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment and government. The international nature of cybercrimes has led to international cyberlaws.

Computer crime or cyber crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft) and electronic fraud[12].

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "*a legal wrong that can be followed by criminal proceedings which may result into punishment.*" The hallmark of criminality is that, it is breach of the criminal law.

---

[9] http://www.wordiq.com/definition/Computer_crime
[10] http://legal-dictionary.thefreedictionary.com/Computer+Crime
[11] http://encyclopedia2.thefreedictionary.com/Computer+Crime
[12] http://www.cyberlawsindia.net/computer-crime.html

Per Lord Atkin "*the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences*".

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime and where either the computer is an object or subject of the conduct constituting crime". *"Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime"*. A generalized definition of cyber crime may be "*unlawful acts wherein the computer is either a tool or target or both*". The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

It is hereby clarified that the terms cybercrimes and computer crimes are synonyms to each other. People use both the terms computer crimes and cyber crimes as interchangeable, but in reality cybercrimes are broader than computer crimes. In case of computer crimes, the computer is the sole tool for committing the crimes but in case of cyber crimes the crimes could be committed, not only, through computers but mobiles, Personal Digital Assistants etc. also. Thus, we can say that all the computer crimes are cyber crimes but all the cyber crimes are not computer crimes.

1.4 KINDS OF COMPUTER CRIMES

According to the http://oreilly.com/catalog/crime/chapter/cri_02.html#41745 , there are following kinds of cyber crimes;

1) **Breaches of Physical Security**
   - i) Dumpster Diving
   - ii) Wiretapping
   - iii) Eavesdropping on Emanations
   - iv) Denial or Degradation of Service

2) **Breaches of Personnel Security**
   - i) Masquerading
   - ii) Social Engineering
   - iii) Software Piracy

3) **Breaches of Communications and Data Security**
   - i) Data Attacks
   - ii) Unauthorized Copying of Data
   - iii) Traffic Analysis

iv) Covert Channels

v) Software Attacks

vi) Trap Doors

vii) Session Hijacking

viii) Tunneling

ix) Timing Attacks

x) Trojan Horses

xi) Viruses and Worms

xii) Salamis

xiii) Logic Bombs

4) **Breaches of Operation Security**

i) Data Diddling

ii) IP Spoofing

iii) Password Sniffing

iv) Scanning

v) Excess Privileges

The Cybercrimes Investigation Cell, Mumbai briefly describes the following cyber crimes[13].

- **Hacking:** Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user.
- **Virus Dissemination:** Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious software)
- **Software Piracy:** Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- Retail revenue losses worldwide are ever increasing due to this crime
- Can be done in various ways:

  End user copying, hard disk loading Counterfeiting illegal downloads from the internet etc.
- **Credit Card Fraud:** You simply have to type credit card number into www page off the vendor for online transaction. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner
- **Net Extortion:** Copying the company's confidential data in order to extort said company for huge amount.
- **Phishing:** It is technique of pulling out confidential information from the bank/ financial institutional account holders by deceptive means.

---

[13] http:/www.cybercellmumbai.com/files/Types%20of%20cyber%20crime.pdf

Example of Phishing e-mail:

From: *****Bank [mailto:support@****Bank.com]

Sent: 08 June 2004 03:25

To: India

Subject: Official information from ***** Bank

Dear valued ***** Bank Customer!

For security purposes your account has been randomly chosen for verification. To verify your account information we are asking you to provide us with all the data we are requesting. Otherwise we will not be able to verify your identity and access to your account will be denied. Please click on the link below to get to the bank secure page and verify your account details. Thank you. https:/ /infinity.*****bank.co.in/Verify.jsp

****** Bank Limited

- **Spoofing:** Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges so as to obtain access to the other computers on the network.
- **Cyber Stalking:** The Criminal follows the victim by sending e-mails entering the chat rooms frequently.
- **Cyber Defamation:** The Criminal sends e-mails containing defamatory matters to all concerned off the victim or post the defamatory matters on a website. (Disgruntled employee may do this against boss, ex-boys friend against girl, divorced husband against wife etc).
- **Threatening:** The Criminal sends threatening e-mail or comes in contact in chat rooms with victim. (Any one disgruntled may do this against boss friend or official).
- **Salami Attack:** In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. Criminal makes such program that deducts small amount like Rs. 2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.
- **Sale of Narcotics:** Sale and Purchase through net.
  - There are web site which offers sale and shipment off contrabands drugs.
  - They may use the techniques off stegnography for hiding the messages.
- **Nigerian 4-1-9 Scam:** This scam starts with a bulk mailing or bulk faxing of a bunch of identical letters to businessmen, professionals and other persons who tend to be of greater-than-average wealth. This scam is often referred to as the 4-1-9 scam, ironically after section 4-1-9 of the Nigerian Penal Code which relates to fraudulent schemes.
- **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.
- **E-mail 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.

- **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.

- **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.

- **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. 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.

- **Harassment via e-mails**

  Harassment through e-mails is not a new concept. It is very similar to harassing through letters. This is a very common type of harassment via e-mails.

- **Dissemination of obscene material/Indecent exposure/Pornography/ Polluting through indecent exposure**

  Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials. Downloading obscene materials through the Internet. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

- **Unauthorized control/access over computer system**

  This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

- **Computer vandalism**

  Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

- **Cyber terrorism**

Cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks, etc. Cyber terrorism may be defined to be "the premeditated use of disruptive activities or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives".

Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to:

1) putting the public or any section of the public in fear; or

2) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

3) coercing or overawing the government established by law; or

4) endangering the sovereignty and integrity of the nation and a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

- **Fraud and Cheating**

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

[14]Computer crimes range from the catastrophic to the merely annoying. A case of computer-driven espionage might wreak devastating losses to national security. A case of commercial computer theft might drive a company out of business. Some computer crimes are perpetrated for kicks and some for social or political causes; others are the serious business of professional criminals. There is perhaps no other form of crime that cuts so broadly across the types of criminals and the severity of their offenses.

In the context of the emerging cybercrimes, there has become an absolute necessity to understand the various kinds of securities that are relevant today in the context of the use of computers, computer systems and computer networks. Let us examine some of these:

- **Physical security**

Protection of the physical building, computer, related equipment and media (e.g. disks and tapes).

- **Personnel security**

Protection of the people who work in any organization and protection of computer equipment and data from these people and others outside the organization.

---

http://oreilly.com/catalog/crime/chapter/cri_02.html#41745

- **Communications security**

  Protection of software and data, especially as it passes from computer to computer.

- **Operations security**

  Protection of the procedures used to prevent and detect security breaches and the development of methods of prevention and detection.

1.5 BREACHES OF PHYSICAL SECURITY

Terrorist bombings on buildings housing computer equipment, arson and theft and destruction of computer equipment fall into this category. You may not realize that less obvious attacks, like turning off the electricity in a computer room, spilling soda on a keyboard and throwing sensitive papers in the trash may also invite disaster.

- **Dumpster Diving**

  Dumpster diving or trashing, is a name given to a very simple type of security attack--scavenging through materials that have been thrown away. Dumpster diving also isn't unique to computer facilities. All kinds of sensitive information turn up in the trash and industrial spies through the years have used this method to get information about their competitors.

  Electronic trashing is easy because of the way that systems typically delete data. Usually, "deleting" a file, a disk or a tape doesn't actually delete data, but simply rewrites a header record. If you are running MS-DOS, for example, you can delete a file via the DEL command; however, someone can retrieve the contents of the file simply by running UNDELETE. System utilities are available that make it easy to retrieve files that may seem to be completely gone. This is sometimes a source of embarrassment.

  Although there are methods for truly erasing files and magnetic media, most computer operators who work on large systems do not take the time to erase disks and tapes when they are finished with them. They may discard old disks and tapes with data still on them. They simply write the new data over the old data already on the tape. Because the new data may not be the same length as the old, there may be sensitive data left for those skilled enough to find it. It is far safer to explicitly write over storage media and memory contents with random data and to degauss magnetic tapes.

- **Wiretapping**

  There are a number of ways that physical methods can breach networks and communications. Telephone and network wiring is often not protected as well as it should be, both from intruders who can physically damage it and from wiretaps that can pick up the data flowing across the wires.

  Telephone fraud has always been a problem among crackers, but with the increasing use of cellular phones, phone calling cards and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years.

- **Eavesdropping on Emanations**

  Electronic emanations from computer equipment are a risk you need to be aware of, although this is mainly a concern for military and intelligence data. Computer equipment, like every other type of electrical equipment from hairdryers to stereos, emits electromagnetic impulses. Whenever you strike a computer key, an electronic impulse is sent into the immediate area. Becau

of the emanation threat, government computers that are used to store and process classified information require special physical shielding. The U.S. federal TEMPEST program is designed to develop, test and certify specially shielded computer equipment from mainframes to terminals to cabling.

There are other types of emissions as well. Criminals have even recorded the noise from a computer printer (the key-and-ribbon variety; it can't be done with laser printers) and then play the recording later to determine which keys were active.

- **Denial or Degradation of Service**

  Some cases of electronic sabotage involve the actual destruction or disabling of equipment or data. Turning off power or sending messages to system software telling it to stop processing are examples of the first type of attack – a classic denial of service.

  The other type of attack, known as flooding (or sometimes wedging or spamming) is the type we saw with the Internet worm. As the worm spread across systems and networks, it kept creating new processes that so clogged the affected systems that other work couldn't get done. In this type of attack, instead of shutting down service, the attacker puts more and more of a strain on the systems' ability to service requests, so eventually they can't function at all.

1.6 BREACHES OF PERSONNEL SECURITY

To some extent, nearly all of the attacks we discuss in this chapter could be considered in the realm of personnel security--after all, people commit the offenses and people ultimately detect them. In fact, many of the crimes we talk about in terms of computer security happen whether or not computers are involve-bribery, subversion, extortion and malicious mischief of all kinds. Only the targets and the media may differ.

Masquerading

Masquerading occurs when one person uses the identity of another to gain access to a computer. This may be done in person or remotely.

There are both physical and electronic forms of masquerading. In person, a criminal may use an authorized user's identity or access card to get into restricted areas where he will have access to computers and data. This may be as simple as signing someone else's name to a sign in sheet at the door of a building. It may be as complex as playing back a voice recording of someone else to gain entry via a voice recognition system

Electronically, an unauthorized person will use an authorized user's logon ID, password and personal identification number (PIN) or telephone access code to gain access to a computer or to a particular set of sensitive data files. There are many ways to obtain this information, some of them quite simple and others quite complex. For example, they might have obtained this information by theft (if the authorized user has written down these numbers and codes), eavesdropping electronically (via password sniffers or other types of monitoring programs) or simply looking over the shoulder of the user while he or she types.

Unauthorized password use is the most common type of electronic masquerading and it's a very effective one.

To understand how masquerading works, you need to know a few basics about how users gain access to shared systems via a two-step process known as identification and authentication.

Identification is the way you tell the system who you are. For example, you enter your user account name in response to a "login" prompt or you enter your bank account number at an ATM machine. Authentication is how you prove to the system that you are who you say you are. There are three classic ways in which you can prove yourself:

Something you know: The most common example is a password or a PIN. The theory is that if you know the password or PIN for an account, you must be the owner of it.

Something you have: Examples are keys, tokens, badges and smart cards that you use to "unlock" a building, a door, a computer or an account.

Something you are or do: Examples are physiological traits, like your fingerprint or voiceprint or behavioral traits, like your signature or keystroke pattern.

Social Engineering

Social engineering is the name given a category of attacks in which someone manipulates others into revealing information that can be used to steal data or subvert systems. Such attacks can be very simple or very complex. In one low-tech case we know about, a man posing as a magazine writer was able to get valuable information over the telephone from the telephone company simply by asking for it--supposedly for his story. He then used that information to steal more than a million dollars in telephone company equipment.

Software Piracy

Software piracy is an issue that spans the category boundaries and may be enforced in some organizations and not in others. Pirated computer programs are big business. Copying and selling off-the-shelf application programs in violation of the copyrights costs software vendors many millions of dollars. The problem is an international one, reaching epidemic proportions in some countries.

1.7 BREACHES OF COMMUNICATIONS AND DATA SECURITY

In this category we include attacks on computer software and on the data itself. The other categories we've discussed in this chapter are more focused on physical equipment, people and procedures.

Data Attacks

There are many types of attacks on the confidentiality, integrity and availability of data. Confidentiality keeps data secret from those not authorized to see it. Integrity keeps data safe from modification by those not authorized to change it. Availability, as we discussed under "Denial or Degradation of Service" above, keeps data available for use.

The theft or unauthorized copying, of confidential data is an obvious attack that falls into this category. Espionage agents steal national defense information. Industrial spies steal their competitors' product information. Crackers steal passwords or other kinds of information on breaking into systems.

Unauthorized Copying of Data

Software piracy, which we discussed in "Breaches of Personnel Security" above, is another attack that spans the categories we've identified in this chapter. In some sense, piracy is just another example of the unauthorized copying of data. The methods for detecting and preventing such a crime are the same whether the copied

data is national defense plans, commercial software or sensitive corporate or personal data.

Preventing and detecting this type of attack requires coordinated policies among the different categories of computer security. In terms of personnel security, user education is vital. In terms of operations security, automated logging and auditing software can play a part as well.

Traffic Analysis

Sometimes, the attacks on data might not be so obvious. Even data that appears quite ordinary may be valuable to a foreign or industrial spy. For example, travel itineraries for generals and other dignitaries help terrorists plan attacks against their victims. Accounts payable files tell outsiders what an organization has been purchasing and suggest what its future plans for expansion may be. Even the fact that two people are communicating--never mind what they are saying to each other–may give away a secret. Traffic analysis is the name given to this type of analysis of communications.

In one industrial espionage case, a competitor monitored a company's use of online data services to find out what questions it had and what information it was collecting on certain types of metallurgy. The information allowed the competitor to monitor the company's progress on a research and development project and to use this information in developing its own similar product. That product reached the market several weeks before the original developer was able to. The original company's research and development investment and its potential share of the market--many millions were all but lost.

Covert Channels

One somewhat obscure type of data leakage is called a covert channel. A clever insider can hide stolen data in otherwise innocent output. For example, a filename or the contents of a report could be changed slightly to include secret information that is obvious only to someone who is looking for it. A password, a launch code or the location of sensitive information might be conveyed in this way. Even more obscure are the covert channels that convey information based on a system clock or other timed event. Information could, in theory, be conveyed by someone who controls system processing in such a way that the elapsed time of an event itself conveys secret information.

Trap Doors

One classic software attack is the trap door or back door. A trap door is a quick way into a program; it allows program developers to bypass all of the security built into the program now or in the future.

Trap doors make obvious sense to expert computer criminals as well, whether they are malicious programmers or crackers. Trap doors are a nifty way to get into a system or to gain access to privileged information or to introduce viruses or other unauthorized programs into the system.

Session Hijacking

Session hijacking is a relatively new type of attack in the communications category. Some types of hijacking have been around a long time. In the simplest type, an unauthorized user gets up from his terminal to go get a cup of coffee. Someone lurking nearby probably a co-worker who isn't authorized to use this particular system sits down to read or change files that he wouldn't ordinarily be able to access.

Sometimes, an attacker will connect a covert computer terminal to a line between the authorized terminal and the computer. The criminal waits until the authorized

terminal is on line but not in use and then switches control to the covert terminal. The computer thinks it is still connected to the authorized user and the criminal has access to the same files and data as the authorized user. Other types of hijacking occur when an authorized user doesn't log out properly so the computer still expects a terminal to be connected. Call forwarding from an authorized number to an unauthorized number is another method of getting access.

Tunneling

Technically sophisticated tunneling attacks fall into this category as well. Tunneling uses one data transfer method to carry data for another method. Tunneling is an often legitimate way to transfer data over incompatible networks, but it is illegitimate when it is used to carry unauthorized data in legitimate data packets.

Timing Attacks

Timing attacks are another technically complex way to get unauthorized access to software or data. These include the abuse of race conditions and asynchronous attacks. In race conditions, there is a race between two processes operating on a system; the outcome depends on who wins the race. Although such conditions may sound theoretical, they can be abused in very real ways by attackers who know what they're doing. On certain types of UNIX systems, for example, attackers could exploit a problem with files known as setuid shell files to gain superuser privileges. They did this by establishing links to a setuid shell file, then deleting the links quickly and pointing them at some other file of their own. If the operation is done quickly enough, the system can be made to run the attacker's file, not the real file.

Trojan Horses

Trojan horses, viruses, worms and their kin are all attacks on the integrity of the data that is stored in systems and communicated across networks. Because there should be procedures in place for preventing and detecting these menaces, they overlap with the operations security category as well.

In the computer world, Trojan horses are still used to sneak in where they're not expected. A Trojan horse is a method for inserting instructions in a program so that program performs an unauthorized function while apparently performing a useful one. Trojan horses are a common technique for planting other problems in computers, including viruses, worms, logic bombs and salami attacks (more about these later). Trojan horses are a commonly used method for committing computer-based fraud and are very hard to detect.

Viruses and Worms

In a computer, a virus is a program which modifies other programs so they replicate the virus. In other words, the healthy living cell becomes the original program and the virus affects the way the program operates. How? It inserts a copy of itself in the code. Thus, when the program runs, it makes a copy of the virus. This happens only on a single system. (Viruses don't infect networks in the way worms do, as we'll explain below.) However, if a virus infects a program which is copied to a disk and transferred to another computer, it could also infect programs on that computer. This is how a computer virus spreads.

Unlike a virus, a worm is a standalone program in its own right. It exists independently of any other programs. To run, it does not need other programs. A worm simply replicates itself on one computer and tries to infect other computers that may be attached to the same network.

Salamis

The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time (hence the name salami). Usually, the amount stolen each time is so small that the victim of the salami fraud never even notices.

Logic Bombs

Logic bombs may also find their way into computer systems by way of Trojan horses. A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage.

Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. In several cases, a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it.

1.8 BREACHES OF OPERATION SECURITY

Data Diddling

Data diddling, sometimes called false data entry, involves modifying data before or after it is entered into the computer. Consider situations in which employees are able to falsify time cards before the data contained on the cards is entered into the computer for payroll computation. A timekeeping clerk in a 300-person company noticed that, although the data entered into the company's timekeeping and payroll systems included both the name and the employee number of each worker, the payroll system used only the employee's number to process payroll checks. There were no external safeguards or checks to audit the integrity of the data. She took advantage of this vulnerability and filled out forms for overtime hours for employees who usually worked overtime. The cards had the hardworking employees' names, but the time clerk's number. Payment for the overtime was credited to her.

In another case, two employees of a utility company found that there was a time lapse of several days between when meter readings were entered into the computer and when the bills were printed. By changing the reading during this period, they were able to substantially reduce their electric bills and the bills of some of their friends and neighbours.

IP Spoofing

In "Breaches of Personnel Security" above, we introduced masquerading attacks, particularly those involving one person pretending to be another. But there are some more complex masquerading attacks that can be prevented only by strong operations security.

A method of masquerading that we're seeing in various Internet attacks today is known as IP spoofing (IP stands for Internet Protocol, one of the communications protocols that underlies the Internet). Certain UNIX programs grant access based on IP addresses; essentially, the system running the program is authenticated, rather than the individual user. The attacker forges the addresses on the data packets he sends so they look as if they came from inside a network on which systems trust

each other. Because the attacker's system looks like an inside system, he is never asked for a password or any other type of authentication. In fact, the attacker is using this method to penetrate the system from the outside.

Password Sniffing

Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password as required when using certain common Internet services like FTP (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine) the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces (e.g. the user names and passwords) and cover up the existence of the sniffers in an automated way.

One-time passwords and encrypted passwords are good ways to keep password sniffing attacks from compromising systems.

Scanning

A technique often used by novice crackers, called scanning or war dialing, also is one that ought to be prevented by good operations security.

Suppose that a computer criminal looks in the telephone book and finds that the telephone numbers for the Fourth National Bank range from 791-0000 to 791-5578. Before he goes to bed one night, he programs his computer to call all of the numbers in this range and to record the ones that are answered by a modem. In the morning, he prints out the successful numbers. He now has a list of the telephone numbers that are most likely to give him access to the bank's computers. The next evening, he dials those numbers and tests his skills as a cracker. With skill, determination and a little luck, he may eventually use these phone numbers as the opening wedge into a bank computer and eventually into some accounts from which he can transfer funds.

Excess Privileges

If a cracker breaks into one user's account, he can compromise and damage that user's files, but he can't ordinarily get beyond the boundaries of the user's account to damage the rest of the system. Or can he? Sometimes, the answer is yes and the reason is that, too often, users in a system have excess privileges more privileges than they ought to have. An ordinary user on an ordinary system doesn't need to be able to modify all of the files on that system. And yet, in many systems, a user has the system privileges that entitle him to do just that. The user may never actually want to change anyone else's files he may not even know that he is allowed to--but nevertheless the privileges are there. If an intruder gets access to the system through the user's account, he can exploit this weakness.

In one case of super zapping, the manager of computer operations in a bank was told by his boss to correct a problem affecting account balances. The problem was originally caused by unanticipated problems in the changeover of the bank's computer system. While working on the project, the manager found that he could use the Superzap program to make other account changes as well, without having to deal with the usual controls, audits or documentation. He moved funds from various accounts into the accounts of several friends, netting about $128,000 in all. He was detected only when a customer complained about a shortage in his account. Because the Superzap program left no evidence of data file changes, the fraud was highly unlikely to be discovered by any other means.

1.9 CASE STUDY IN CYBER CRIMES

There are various computer crimes which has been committed since the advent of computer and internet. But all the crimes relating to internet and computers have not come to the knowledge of people. There are few cases where the victims of computer crimes initiated the legal proceeding, otherwise the rest of the cased are unreported and have not become the part of the public domain.

Let us now examine some cases, which have been reported in the public domain, which relate to cybercrimes as also contraventions of the laws prevailing for the time being in place in the relevant jurisdictions :

A) Cubby, Inc vs. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y.1991)

CompuServe is an online company providing access to over 150 special interest forums comprised of electronic bulletin boards, interactive online conferences and topical databases. A newsletter called Rumorville was made available via the bulletin board. The plaintiff sued CompuServe for libel after allegedly defamatory statements were disseminated through the newsletter against it. It was argued that the court should consider CompuServe to be a "publisher" of the allegedly defamatory statements and thus hold it liable for the statement.

The court held that CompuServe had "no more editorial control over such a publication than does a public library, bookstore or newsstand". The court instead found CompuServe to be more akin to a "distributor" rather than a "publisher". Thus, because it was undisputed that CompuServe did not have knowledge of or reason to know of the allegedly defamatory statements made in the publication, especially given the large number of publications it carries and the speed with which publications are uploaded into its computer banks and made available to CompuServe subscribers, the court held that CompuServe could not be held liable to Cubby for the defamatory statements. The court noted that to impose on CompuServe the duty to examine every publication it carries for defamatory statements would "impose an undue burden on the free flow of information".

B) Groff vs. America Online, Inc., 1998 WL 307001 (1998)

The plaintiff, an individual in Rhode Island who subscribed to America Online, sued the company in Rhode Island state court, alleging violations of state consumer protection legislation. The process of becoming a member of AOL includes a step in which the applicant must assent to AOL's terms of service by clicking an "I Agree" button. The terms of service "contains a forum-selection clause which expressly provides that Virginia law and Virginia courts are the appropriate law and forum for the litigation between members and AOL." AOL moved to dismiss this suit from the Rhode Osland Superior Court for improper venue on the ground that a forum selection clause in the parties' contract mandated that the suit be brought in Virginia, where AOL's base of operations was located. The court agreed and dismissed the suit.

The court held that the plaintiff assented to AOL's terms of service online by the click of an "I agree" button. The terms of service included a clause mandating that suits concerning the service be brought in Virginia. AOL customers must first click on an "I agree" button indicating assent to be bound by AOL's terms of service before they can use the service. This button first appears on a web page in which the user is offered a choice either to read or simply agree to be bound by, AOL's terms of service. It also appears at the foot of the terms of service, where the user is offered the choice of clicking either an "I agree" or "I disagree" button, by which he accepts or rejects the terms of service. The court held that a valid contract existed, even if the plaintiff did not know of the forum selection clause:

"Our Court stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively "signed" the agreement by clicking. "I agree not once but twice." Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."

C) State Bank of India vs. Rizvi Exports Ltd, II (2003) BC 96 (Debt Recovery Appellate Tribunal, Allahabad)

State Bank of India (SBI) (Appellants) had filed a case to recover money from some persons who had taken various loans from it Respondent: Rizvi Exports Ltd. As part of the evidence, SBI submitted printouts of statement of accounts maintained in SBI's computer systems.

As the relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts, the Court held that these documents were not admissible as evidence.

D) Diebold Systems Pvt Ltd vs. The Commissioner of Commercial Taxes., [2006] 144 STC 59 (Kar)

Diebold Systems Pvt Ltd Appellants manufactures and supplies Automated Teller Machines (ATM). Diebold sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of Automated Teller Machines.

The majority view of the ARA was to classify ATMs as "computer terminals" liable for 4% basic tax as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of electronic goods, parts and accessories thereof. They would thus attract basic rate of tax of 12% and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals. Findings of the court

1) The enlarged definition of "computers" in the Information Technology Act cannot be made use of interpreting an Entry under fiscal legislation.

2) An Automatic Teller Machine is an electronic device, which allows a bank's customer to make cash withdrawals and check their account balances at any time without the need of human teller.

3) ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by the person using ATM's. The computer is connected electronically to many ATM's that may be located from some distance from the computer. Decision of the court Decided On: 31.01.2005 was thatATMs are not computers, but are electronic devices under the Karnataka Sales Tax Act, 1957.

E) Ritu Kohli Case[15]

Ritu Kohli Case, being India's first case of cyber stalking, was indeed an

[15] http://www.cyberlawindia.com/casestudies2.php

important revelation into the mind of the Indian cyber stalker. A young Indian girl being cyber stalked by a former colleague of her husband, Ritu Kohli's case took the imagination of India by storm. The case which got cracked however predated the passing of the Indian Cyber law and hence it was just registered as minor offences under the Indian Penal Code.

F) Avnish Bajaj vs. State (N.C.T.) of Delhi, (2005) 3 Comp, LJ 364 (Del), 116(2005)DLT427, 2005(79)DRJ576.

Avnish Bajaj (Appellants), CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website. The court granted him bail in the case on.

Factors considered by the court were:

1) There was no prima facie evidence that Mr. Bajaj directly or indirectly published the pornography,

2) The actual obscene recording/clip could not be viewed on Baazee.com,

3) Mr. Bajaj was of Indian origin and had family ties in India.

History of the case:

Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale. Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

Issues raised by the Prosecution

1) The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.

2) The item description "DPS Girl having fun" should have raised an alarm.

Issues raised by the Defence

1) Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.

2) On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

Findings of the court

1) It has not been established from the evidence that any publication took place by the accused, directly or indirectly.

2) The actual obscene recording/clip could not be viewed on the portal of Baazee.com.

3) The sale consideration was not routed through the accused.

4) Prima facie Baazee.com had endeavored to plug the loophole.

5) The accused had actively participated in the investigations.

6) The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.

7) Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

8) The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.

9) The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person. Decision of the court given on 21.12.2004:

   1) The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.

   2) The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

   3) The court also ordered Mr. Bajaj to participate and assist in the investigation.

G) State of Maharashtra vs. Anand Ashok Khare[16]

This case related to the activities of the 23-year-old Telecom engineer Anand Ashok Khare from Mumbai who posed as the famous hacker Dr Neuker and made several attempts to hack the Mumbai police Cyber Cell website.

H) State of Tamil Nadu vs. Dr L. Prakash[17]

State of Tamil Nadu vs. Dr L. Prakash was the landmark case in which Dr L. Prakash was sentenced to life imprisonment in a case pertaining to online obscenity. This case was also landmark in a variety of ways since it demonstrated the resolve of the law enforcement and the judiciary not to let off the hook one of the very educated and sophisticated professionals of India.

I) Benususan Restaurant Corp. vs. King, 937 F.Supp. 295 (SDNY, 1996)

A New York jazz club operator sued a Missouri club owner claiming trademark infringement, dilution and unfair competition over the use of the name "The Blue Note". The defendant maintained a web site promoting his Missouri "Blue Note" club and providing a Missouri telephone number through which tickets to the club could be purchased.

The issue, as framed by the Federal District Court, was whether the existence of the web site, without more, was sufficient to vest the court with personal jurisdiction over the defendant under New York's long-arm statue. The court held that it did not. The court considered whether the existence of the web site and telephone ordering information constituted an "offer to sell" the allegedly infringing "product" in New York and concluded it was not. The court noted that, although the web site is available to any new Yorker with Internet access, it takes several affirmation steps to obtain access to this particular site, to utilize the information contained there and to obtain a ticket to the defendant's club.

[16] http://www.cyberlawindia.com/casestudies2.php

[17] http://www.cyberlawindia.com/casestudies2.php

J) Ashcroft, Attorney General et al vs. Free Speech Coalition, et al., No 00-795

The US Supreme Court affirmed the judgment of the Court of Appeals for the Ninth Circuit that the prohibitions of Ss.2256 (8)(B) and 2256(8)(D) are overboard and unconstitutional. Being part of the Child pornography prevention Act of 1996 (CPPA) S. 2256 (8) (B) bans a range of sexually explicit images, sometimes called "virtual child pornography," that appear to depict minors but were produced by means other than using real children, such as through the use of youthful-looking adults or computer-imaging technology and S.2256(8)(D) is aimed at preventing the production or distribution of pornographic material pandered as child pornography.

Justice Kennedy opinion:

"Congress may pass valid laws to protect children from abuse and it has. The prospect of crime however, by itself does not justify laws suppressing protected speech."

As a general principle, the First Amendment bars the government from dictating what see or read or speak or hear. The freedom of speech has its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity and pornography produced with real children.

The Government submits."That virtual child pornography whets the appetites of pedophiles and encourages them to engage in illegal conduct. This rationale cannot sustain the provision in question. The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it. The government "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts." First Amendment freedom is most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom and speech must be protected from the government because speech is the beginning of thought." (Decided on April 16, 2002)

K) State vs. Amit Prasad[18]

State vs. Amit Prasad, was India's first case of hacking registered under Section 66 of the Information Technology Act 2000. A case with unique facts, this case demonstrated how the provisions of the Indian Cyber law could be interpreted in any manner, depending on which side of the offence you were on.

L) R vs. Graham Waddon., Southwark [Crown Court, 30/6/1999]

The defendant was charged with numerous counts of publishing obscene articles contrary to S. 2(1) of UK's Obscene Publications Act 1959. The defendant had created pornographic images, which were illegal under the UK's Obscene Publications Act. He ran a series of sites based in the US, hosting them on a US based Internet service provider. These images were accessible to anyone in the world via the Internet who became a subscriber by giving credit card details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could log onto the various websites to obtain the images. It was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore the instant court did not have jurisdiction.

[18] http://www.cyberlawindia.com/casestudies2.php

Hardy Christopher, J. held

"Publishing an article under S. 1(3)(b) of the 1959 Act included data stored electronically and transmitted. To transmit simply meant to send from one place or person to another. In the instant case, an act of publication took place when the data was transmitted by the defendant or his agent to the service provider and the publication or transmission was in effect still taking place when the data was received. Both the sending and receiving took place within the jurisdiction of the court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving".

M) Syed Asifuddin and Ors. vs. The State of AP. & Anr., 2005CriLJ4314

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Case Details: Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500/- as well as service bundle for 3 years with an initial payment of Rs. 3350/- and monthly outflow of Rs. 600/-. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically "unlocked" so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this "unlocking" by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for reprogramming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defense in the case:

1) It is always open for the subscriber to change from one service provider to the other service provider.

2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1

or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4) A telephone handset is neither a computer nor a computer system containing a computer programmed.

5) There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Courts Observation:

1) As per section 2 of the Information Technology Act, a computer is any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2) The instructions or programmed given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4) When the person moves from one cell to another cell in the same city, the system i.e. Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's

location in a database, knows which cell phone you are using and gives a ring.

12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Court Decided On: 29.07.2005

1) A cell phone is a computer as envisaged under the Information Technology Act.

2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –

   a) "when the computer source code is required to be kept"

   b) "maintained by law for the time being in force"

N) Arif Azim case[19]

Arif Azim case was India's first convicted cyber crime case. A case pertaining to the mis-use of credit cards numbers by a Call Center employee, this case generated a lot of interest. This was the first case in which any cyber criminal India was convicted. However, keeping in mind the age of the accused and no past criminal record, Arif Azim the accused was sentenced to probation for a period of one year.

O) The Air Force Bal Bharti School case[20]

The Air Force Bal Bharti School case demonstrated how Section 67 of the Information Technology Act 2000 could be applicable for obscene content created by a school going boy.

P) P.R. Transport Agency through its partner Sri Prabhakar Singh Vs. Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat

---

[19] http://www.cyberlawindia.com/casestudies2.php

[20] http://www.cyberlawindia.com/casestudies2.php

Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director., Writ Petition No. 58468 of 2005

History of the case

Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery. The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC.

BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programmed or feeding of data the higher bid had not been considered earlier. This communication was challenged by PRTA in the High Court of Allahabad.

BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

Issue raised by BCC

The High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P.

Issues raised by PRTA

1) The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action".

2) The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Observation by the court:

1) In reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points.

2) In case of e-mail, the data (in this case acceptance) can be transmitted from any where by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt.

3) Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "...an electronic record is deemed to be received at the place where the addressee has his place of business."

4) The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

Decision of the court Decided On: 24.09.2005

1) The acceptance was received by PRTA at Chandauli/Varanasi. The contract became complete by receipt of such acceptance.

2) Both these places are within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action has arisen in U.P. and the court has territorial jurisdiction.

Q) Washington Post vs. Total News, 97 CIF. 1190 (PKL)

In this case, the "totalnews.com" website used framing technology to set a news story from other website within the overall Total News frame by blocking banner advertisements and other distinguishing features.

The U.S. District Court Southern District of New York passed an order of settlement stating that "the defendants agree permanently to cease the practice of framing plaintiff's websites". Plaintiffs agree that Defendants may link from the Totalnews.com website or any other website to any plaintiff's website, provided that:

a) Defendants may link to plaintiff's website only via hyperlinks consisting of the names of the linked sites in plain text, which may be highlighted;

b) Defendants may not use on any website, as hyperlinks or in any other way, any of plaintiff's proprietary logos or other distinctive graphics, video or audio material, nor may defendants otherwise link in any manner reasonably likely to:

   i) imply affiliation with, endorsement or sponsorship by any plaintiff;

   ii) cause confusion, mistake or deception;

   iii) dilute Plaintiff's marks; or

   iv) otherwise violate state or federal law;

c) Each plaintiff's agreement to permit linking by defendants remains revocable, on 15 business days notice, at each Plaintiff's sole discretion. Revocation by any plaintiff shall not affect any other terms and conditions set forth herein. If defendants refuse to cease linking upon notice and any plaintiff brings an action to enforce its rights under this subparagraph, it shall be an affirmative defense that defendants conduct does not otherwise infringe or violate plaintiffs rights under any theory of any intellectual property, unfair competition or other law.

R) Umashanker vs. ICICI Bank Petition No. 2462 of 2008

The Adjudicator of Tamil Nadu jolted Indian Bankers out of their cozy slumber by his decision on April 12, 2010 in the case of Umashankar Sivasubramaniam Vs ICICI Bank. In this case, the adjudicator PWC Davidar held ICICI Bank liable to pay damages to the extent of Rs 12.85 lakh on an alleged "phishing" fraud incident involving fraudulent transfer of an amount of Rs 6.46 lakh. In the ICICI Bank phishing fraud case, the Adjudicator clearly documented reasons why he considers it necessary to hold the bank liable not only to repay the involved amount, but also interest and other expenses.

S) Pooja Chandrakant Darooka vs. Shri Nainesh Dharmeshbhai Modi Ors No. SCA/10/2010/45794/IT

The respondents misguided the applicant for approving a car loan from various banks. Respondents misguided the applicant that credit card and debit card details are must for income tax return filing and for the faster processing of a

car loan. They played various social engineering techniques with Applicant and collected credit cards, debit cards and related confidential details of the applicant and performed below mentioned unauthorized transactions. Later both respondents realized the seriousness of cyber frauds they committed and Respondent 2 had provided a cheque of Rs.80, 000 on behalf of both the respondents. Later Applicant presented the same cheque 4 times to the bank for clearing but it was returned every time.

The Adjudicating officer, Gujarat has held thus:

Compensation of Rs. 85,000 for the Petitioner is granted considering the financial losses, opportunity losses, business relation and reputational losses with banks, legal expenses and other overheads mentioned in the complaint based on the confessing statements of both the respondents by the Office of Adjudicating officer. Both the Respondents agreed to pay equal amount of the aforesaid compensation to the Petitioner. Advocate for Petitioner also agreed to receive Rs.85,000 as a compensation under section 43 of I.T.Act,2000. Both the parties provided their consents on the aforesaid amount of compensation and decided to put a complete end to the matter before the office of Adjudicating officer and every other authority.

17. Respondents requested the office for some instalment facilities for the payment of aforesaid compensation amount. Advocate & Cyber law Consultant for the petitioner agreed for the same and accordingly Adjudicating officer allowed 5 monthly instalments for the respondents starting from the month of September to the month of January. Both the respondents are informed to deposit 10 cheques in the favour of petitioner in the office of Adjudicating Officer, Gandhinagar on 27.08.2010. Both the parties have deposited the 5 number of cheques as under in favour of the complainant and acoordingly it has been directed to hand over the original cheques as above worth of rupees stated in the above statement to the petitioner for further encashment agreed by the respondents

T) State of Uttar Pradesh vs. Saket Sanghania[21]

This case which was registered under Section 65 of the IT Act, related to theft of computer source code. Saket Singhania an engineer, was sent by his employer to America to develop a software program for the company. Singhania, instead of working for the company, allegedly sold the source code of the programme to an American client of his employer person to which his employer suffered loss

U) The State of Tamil Nadu vs. Suhas Katti[22]

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.

---

[21] http://www.cyberlawindia.com/casestudies2.php

[22] http://www.cyberlawindia.com/casestudies2.php

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.

Honourable Sri.Arulraj, 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 aforesaid cases are some of the case studies that demonstrate various aspects of the legalities attached with different kinds of cybercrimes and other contraventions of the laws impacting activities in cyberspace.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain Computer crime.

.....

.....

.....

.....

2) What are the types of cyber crimes?

.....

.....

.....

.....

3) Write short note on "Breaches of communications and data security".

.....

.....

.....

.....

1.10 LET US SUM UP

This unit deals with computer crime or cyber crime which refers, to criminal exploitation of the Internet. Computer crime includes traditional criminal acts committed with a computer, as well as new offenses that lack any parallels with non-computer crimes. Cyber crime is the latest and perhaps the most complicated

problem in the cyber world. Cyber crimes mainly divided into breaches of physical security, personnel security, communications and data security and operation security.

1.11 CHECK YOUR PROGRESS: THE KEY

1) Computer crime or cyber crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft) and electronic fraud.

2) i) Breaches of Physical Security
   - Dumpster Diving
   - Wiretapping
   - Eavesdropping on Emanations
   - Denial or Degradation of Service

   ii) Breaches of Personnel Security
   - Masquerading
   - Social Engineering
   - Software Piracy

   iii) Breaches of Communications and Data Security
   - Data Attacks
   - Unauthorized Copying of Data
   - Traffic Analysis
   - Covert Channels
   - Software Attacks
   - Trap Doors
   - Session Hijacking
   - Tunneling
   - Timing Attacks
   - Trojan Horses
   - Viruses and Worms
   - Salamis
   - Logic Bombs

   iv) Breaches of Operation Security
   - Data Diddling

- IP Spoofing
- Password Sniffing
- Scanning

3) Refer to Section 1.7

UNIT 2 CONVENTIONAL CRIMES THROUGH COMPUTER

Structure

2.0 INTRODUCTION

The concept of crime is not a modern one but it has been existing from time immemorial. But time to time, the concept and nature of crimes have changed. And the definition of crimes has been changed accordingly. In the era of 20th century and with the advent of computer, the criminals have changed the mode of committing the crimes from conventional methods to computer based methods.

The cyber criminals are totally different from the conventional criminals. Cyber criminals are intellectual, educated and high profiles personalities, unlike the conventional criminals who are uneducated, weak and poor. Cyber criminals use computer, computer resources and computer networks and communication devices as the weapon for committing their crimes, whereas conventional criminals use arms and ammunition, knives and others deadly weapons for committing the crimes. In case of cyber crimes, it is very difficult for law enforcement agencies to prosecute the criminals unlike the conventional crimes.

2.1 OBJECTIVES

After going through this Unit, you should be able to:

- know the history of cyber crimes;
- understand the different cyber crimes; and
- understand the provisions of IPC in the information technology.

2.2 HISTORY OF CYBER CRIMES

In today's era, various conventional crimes are being committed through computers and computer resources.

The first recorded cyber crime[1] took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

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

Today, computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second.

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications. Major cyber crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland.

Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as e-mail spoofing and cyber defamation, sending threatening e-mails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

2.3 MEANING OF CRIMES

The term "Crimes" has, nowhere been defined in the penal law. Section 40 of Indian Penal Code, 1860 defines the terms "offence" as a thing made punishable by this Code.

Wikipedia defines the term "crimes" as Crime is the breach of rules or laws for which some governing authority (via mechanisms such as legal systems) can ultimately prescribe a conviction.

A normative definition views crime as deviant behavior that violates prevailing norms – cultural standards prescribing how humans ought to behave normally. This approach considers the complex realities surrounding the concept of crime

[1] http://hubpages.com/hub/Cyber-Crime

and seeks to understand how changing social, political, psychological and economic conditions may affect changing definitions of crime and the form of the legal, law-enforcement and penal responses made by society[2].

2.3.1 Essentials Elements for Crimes

In the Indian Penal Code, the term "crime" has not been defined but Section 40 of the Indian Penal Code defined the term "offence" as "the thing which is punishable under the Code, is an offence".

There are two essential elements of crimes which are as follows:

i) Actus Reus

ii) Mens Rea

For the purpose of conviction of criminals, the prosecution must prove that the person who has alleged to commit the crime has actus reus and mens rea, as in case of absence of any of the element, the act does not constitute the crime.

It is further pertinent to point out that Indian Penal Code provides that there are certain exceptions, where one of the elements is sufficient to constitute the crime such as, Conspiracy. Under this offence for the purpose of conviction there is a need not to prove both, actus reus and mens rea. Mens rea is sufficient for the conviction of the accused for the offence of conspiracy. On the other hand, there are certain offences where actus rea is sufficient to constitute the crime. There is no need to prove the mens rea i.e. traffic rule. In this case, if the accused violates the traffic rules, he shall be punished accordingly, it is immaterial that there is mens rea or not.

2.3.2 Conventional Crimes[3]

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

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

In the other words, Conventional crimes are those traditional, illegal behaviors that most people think of as crime. Most crime is conventional crime. Non-conventional crime may be organized crime, white-collar crime, political crime etc.

According to this perspective, the probability of criminal victimization varies by time, space and social setting and by the extent to which routine activities increase target suitability and reduce effective guardianship. The patterns and correlates of conventional crimes are consistent with this approach. Crimes against property tend to be committed disproportionately against those whose lifestyle leave their possessions least effectively guarded. Crimes against persons have some different correlates than do crimes against property, but most of these differences are consistent with the lifestyle/exposure theory. For typical crimes, victims (and offenders) are most likely to be young, male and engage in evening activities away from home. Thus, their lifestyles place them in social settings with a higher risk of criminal victimization.

---

[2] http://en.wikipedia.org/wiki/Crime

[3] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

2.4 KINDS OF CONVENTIONAL CRIMES

[4]The International Crime Victim Survey has attracted growing interest from the research community and policy makers. In addition to providing an alternative source of data on crime to complement official statistics, the Survey offers internationally standardized indicators for the perception and fear of crime. At the country level, the International Crime Victim Survey is used to monitor differences in crime and perceptions between countries and over time. By collecting social and demographic information on respondents, crime surveys also allow analysis of how both objective and subjective risks of crime vary for different groups within the population, in terms of age, gender, education, income levels and lifestyles. Data from recent sweeps of the Survey are presented in order to analyse global crime levels and trends.

Generally there are various kinds of conventional crimes i.e. crimes against property, crimes against person, crimes against society, crimes against government or state etc. White collar crime or economic crime could take different forms, including bribery, cyber crime, asset misappropriation, cheque and credit card fraud, identity theft, insurance fraud, money laundering and counterfeiting.

The other main contributing offences are criminal breach of trust, cheating, forgery and illegal money lending. Apart from this, 'occupational crime' to illegal and unethical activities committed for individual financial gain – or to avoid financial loss – in the context of a legitimate occupation.

The term 'occupational deviance' is better reserved for deviation from occupational norms (e.g. drinking on the job; sexual harassment) and the term 'workplace crime' is better reserved for conventional forms of crime committed in the workplace (e.g. rape; assault).

2.5 CYBER CRIME

It has been said that cybercrime is just a conventional crime committed with high-tech devices[5].

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

A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both" The computer may be used as a tool in the following kinds of activity financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Pavan Duggal, Asia's and India's foremost expert on cyberlaw and Advocate, Supreme Court of India has stated at http://www.cyberlaws.net/cyberindia/cybercrime.html as follows:

[4] http://sociologyindex.com/conventional_crime.htm
[5] http://sociologyindex.com/conventional_crime.htm

There can be no one exhaustive definition about Cybercrime. However, any activities which basically offend human sensibilities, can also be included in its ambit. Child Pornography on the Internet constitutes one serious Cybercrime. Similarly, online pedophiles, using internet to induce minor children into sex, are as much Cybercriminals as any other.

Cybercrimes can be basically divided into 3 major categories being Cybercrimes against persons, property and Government.

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail and cyber-stalking.

The trafficking, distribution, posting and dissemination of obscene material including pornography, indecent exposure and child pornography, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be overstated. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

Similarly, Cyber harassment is a distinct Cybercrime. Various kinds of harassment can and does occur in cyberspace or through the use of cyberspace. Harassment can be sexual, racial, religious or other. Persons perpetuating such harassment are also guilty of cybercrimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the precious and extremely touchy area of his or her own privacy which the medium of internet grants to the netizens.

Another Cybercrime against persons is that of Cyberstalking. The Internet is a wonderful place to work, play and study. The Net 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 and harassments are problems that many persons, especially women, are familiar with in real life. These problems also occur on the Internet, in what has become known as "Cyberstalking" or "on-line harassment".

The second category of Cybercrimes is that of Cybercrimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs and unauthorized possession of computerized information.

Hacking and cracking are amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this, the actuality is that no computer system in the world is hacking proof. It is unanimously agreed that any and every system in the world can be hacked. Using one's own programming abilities as also various programmes with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programs or virii which do irreparable damage to computer systems is another kind of Cybercrime. Software piracy is also another distinct kind of Cybercrime which is perpetuated by many people online who distribute illegal and unauthorised pirated copies of software.

The third category of Cybercrimes relate to Cybercrimes against Government. Cyber Terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

2.6 DEVELOPMENT OF CYBER CRIMES

Today, computer has become an instrument for the commission of crimes. These crimes are known as cyber crimes which are different from those conventional crimes defined under Indian Penal Code or enactments like they are committed by obtaining a password and use it in a computer in an unauthorized way. It can also be committed by using software and send the computer virus to other computers.

Cyber Crime is the most recent type of crime which has become biggest challenge for police and prosecution. Tempering with source code, hacking into computer system, publishing obscene information like pornography are the current example of cyber crime[6].

"The concept of cyber crime is not radically different from that of conventional crime," says in a report on the portal, "Both include conduct whether act or omission, which cause breach of rules of law and [are] counterbalanced by the sanction of the state."

However, despite the similar legal nature of both conventional and cyber crime, they are substantially different in practice. Cyber crimes are far easier to learn how to commit, require fewer resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present in and until recently, their status of illegality has been, at best, vague. As the global technology policy and management consulting firm McConnell Institute notes in a comprehensive report on the subject, many countries' existing archaic laws threaten the global information dynamic. "The growing danger from crimes committed against computers or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes".

Cyber Crime is any crime that involves computer or computer system either as a target or as a medium. With this definition, one could/should not be mistaken into thinking that cyber crime only takes place when a computer genius manages to interfere with a networked computer system, bypassing complicated security, encryption or any access-controlling mechanism.

Cyber Crime includes those 'conventional crimes' in which the criminal has found a new way to launch their wrong-doing by way of computer network or otherwise being facilitated by information technologies The legal role of addressing and curbing cyber crime can therefore be attributed to the conventional law of crime[7].

[8]Cyber Crime has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state .particularly those surrounding hacking, copyright infringement through warez, child pornography and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

There are two basic types of cyber crimes. One in which computers themselves are targets (such as criminal data access, data damage, malicious code and various other kinds of information theft on computer networks), while the other in which computer and other technology are used as a tool to commit virtual versions of various conventional crimes (such as cyber terrorism, electronic fraud and forgery, cyber stalking and spamming etc).

[6] http://ezinearticles.com/?Cyber-Crime-Law-Separating-Myth-From-Reality&id=1117070

[7] 7http://sonnyzulhuda.wordpress.com/2010/08/24/penal-code-for-cyber-crime/

[8] 8http://www.seminarprojects.com/Thread-cyber-crime-full-report

India has laws against cybercrimes such as using the Internet to harm minors. The government of India is aware of a new generation of crime brought on by the digital revolution. In 2000, it enacted the Information Technology Act and revised it in 2008 to bring it in line with current issues in cyberspace. Cybercrimes such as child pornography, identity theft, Internet fraud and destruction of property or data are illegal in India; perpetrators face both civil and criminal penalties when they are caught.

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

Laws Enforced Under Indian Penal Code: India has separate laws regarding cybercrime, but violators are generally prosecuted under the Indian Penal Code or IPC, instead of the Information Technology Act of 2000. For example, a person who commits Internet fraud is often prosecuted under the IPC for real-time fraud. Indian law enforcement personnel reason that most cybercrimes have real-time counterparts that are already illegal and it is easier to prosecute for these crimes than for cybercrimes. Fraud, theft, destruction of property and child pornography is all covered by the IPC. Cybercrimes are generally punishable by fines under the Information Technology Act, although perpetrators are also subject to imprisonment under the IPC[9].

The Information Technology Act has added a new word, cyber crimes, which covers various kinds of computer and Internet related crimes, which can be classified into the following heads[10]:

a) Hacking without any intention to commit any further offence or crime.

b) Unauthorized access with intention to commit further offence. These can include theft, fraud, misappropriation, forgery, nuisance tempering with source code, publishing of information which is obscene in electronic form etc.

c) Destruction of digital information through use of Virii.

Hacking is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. The real tangible threat of hacking comes in when an unauthorized access to a system is done with the intention of committing further crimes like fraud, misrepresentation, downloading data in order to commit infringement of copyright, accessing sensitive and top secret data from defence sites etc. Some of the most common types of fraud as committed on the net include bogus online investment newsletters, which give a biased and untrue advice on stocks and securities thereby fictionally giving a pull to the share value of bogus companies etc.

In applying the section to hacking on the Internet, the prime question that needs to be answered is as to whether website is a property. For this it is imperative to consider the computer or the virtual area of the net as a property. Thus, as trespass actions are grounded in the idea of protecting the owners control over real property, there is no inherent reason as to why the owners control over a websites could not be considered as species of property subject to trespass. It is for this reason that hacking is made a crime punishable under Section 66 (2) of the Information Technology Act, 2000 providing for an imprisonment up to 3 years or with fine up to Rs. 5 lacs or with both.

---

[9] http://www.ehow.com/list_6779023_laws-cyber-crime-india.html#ixzz1Ermw1jwh

[10] http://www.articlealley.com/article_99774_18.html

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

Section 25 of the Indian Penal Code defines 'Fraudulently' as an action or deed done with an intention of deceit. The two main ingredients to be satisfied are 'Deceit' or an 'Intention to deceit' and either actual injury or possible injury or an intent to expose some person to actual or possible injury.

Internet fraud is a form of white-collar crime whose growth is as rapid and diverse as the growth of the Internet itself. In fact, the diversity of areas in which the Internet is being used to do fraud people and organization is astonishing. While there are innumerable scams and frauds going on, on the Internet, many of them relate to investments.

2.6.1 Virii in the Light of the Provisions of the IPC

The offence of deliberately and malafidely destroying or altering the data bases of alien computers may best be described as 'Mischief' as defined in sections 425 to 440 of the Indian Penal Code. The essential ingredients for the offence of Mischief being

a) wrongful loss or damage to the public or any person

b) intention to cause such damage or knowledge that such damage or loss might be caused.

c) destruction of property or such alteration to such property as may render it useless or diminishes its value and/or utility.

Virii are self-replicating programs, which on entering a system attach themselves to the digital data of the host computer, thereby destroying and/or altering it and/or rendering it beyond comprehension and making it useless. Computer Virii transfer from computer to computer by disguising themselves as harmless E-mail or any other such thing thereby infecting and destroying the data of the recipient computer as well. The law dealing with Cyber crimes has now been codified in the I. T. Act, 2000 and Chapter XI deals with computer crimes and provide for punishments for these offences.

Another area of cyber crime is with regard to defamation and the Internet. There are various issues related to Internet defamation. These include question of jurisdiction and also questions relating to lack of legal awareness amongst people using the Internet.

An essential ingredient for Defamation as defined under section 499 of the Indian Penal Code is 'Publication'. One of the important business of the Internet is computer software. The issue of computer software piracy is itself not a new one.

However, the issue, which arises out of having computer software on the Internet, is the manner in which piracy is done, the rights and liabilities of various parties involved in the process and the steps taken to curb it. In India, computer software falls under copyright laws and therefore, the software can be protected under the Copyright Act. Cyber squatting as an offence relates to the registration of a domain name by an entity who does not have an inherent right or a similar or identical trade mark registration in it's favor, with the sole view and intention to sell them to the legitimate user in order to earn illegal profits.

In the judgment passed by the Delhi High court in Yahoo! Inc. vs Akash Arora 1999 PTC 201, the court has restrained the defendant from using the Domain name yahooindia.com on the ground that it violated the rights of the plaintiff who was the owner of the domain name yahoo.com.

In Rediff Communications vs Cyberbooth, the defendants were restrained from using the domain name radiff .com as it was deceptively similar to the Plaintiff's registered domain name rediff.com.

The internet and internet related crimes are increasing at an alarming rate. The laws that we are presently trying to fit into the modern scenario, answer some questions but leave twice the number unanswered. The loopholes left by the existing penal provisions make Internet a virtual haven for cyber criminals to carry on their illegal activities unchecked.

In all the crimes examined in this chapter, there is one fundamental aspect that poses serious difficulties. This is the question of jurisdiction. The nature of Internet is such that geographical and political boundaries have been rendered irrelevant. A person with access to a computer and the Internet might be participating, attempting or planning a criminal act anywhere in the world.

2.7 REASONS FOR CYBER CRIME

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

Capacity to store data in comparatively small space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much more easier.

- **Easy to access**

  The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

- **Complex**

  The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

- **Negligence**

  Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

[11] https://sites.google.com/site/cybercrimezbd/reasons-for-cyber-crime

- **Loss of evidence**

  Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

- **Cyber criminals**

  Cyber criminals constitute of various groups/categories. Ranging from children to teenagers to professional cybercrimes, the army of what constitutes cybercriminals continue to expand with each passing day.

2.8 DISTINCTION BETWEEN CONVENTIONAL AND CYBER CRIME

[12]Cyber Crime is any crime that involves computer or computer system either as a target or as a medium. With this definition, one could/should not be mistaken into thinking that cyber crime only takes place when a computer genius manages to interfere with a networked computer system, bypassing complicated security, encryption or any access-controlling mechanism.

Cyber crime includes those 'conventional crimes' in which the criminal has found a new way to launch their wrong-doing, by way of computer network or otherwise being facilitated by information technologies. The legal role of addressing and curbing cyber crime can therefore be attributed to the conventional law of crime.

In fact, while there are not many cases of cyber crime can be successfully enforced using the more-specific cyberlaw, such as Computer Crimes Act, Penal Code (and other conventional law such as on gambling) had come to the rescue. Malaysian authorities had in the past invoked the Penal Code against diverse types of cyber crimes. Some few of those cases are being shared here:

1) **Online Gambling: "Horse betting ring busted" (The Star, 23/1/2007)**

Two foreigners, along with seven local men, have been arrested for illegally operating online horse race gambling with stakes of up to RM600, 000 a week. Johor Baru (South) OCPD Asst Comm Shafie Ismail said initial investigations revealed that the syndicate processed online horse-racing bets three times a week, accepting bets worth RM200, 000 each time.

2) **Online Porn: "Internet Porn: Guard Gets 6 Months Jail" (Bernama, 4/6/2010)**

A security guard was sentenced to six months imprisonment by the KL Sessions Court after he changed his plea to guilty to six charges of peddling pornography on the Internet.

Shahrom Mahadi (45) admitted to 6 counts of uploading pornographic pictures and disseminating them on six websites. He was charged under sec. 292 of the Penal Code, which provides for jail of not more than three years or fine or both, if convicted.

The court was of the view that the jail sentence was appropriate in view of the gravity of the offence and the profit motive involved. The court found that the websites were deliberately set up to get clients which pose a severe danger to impressionable youngsters. The six-month jail sentences for each of the counts were ordered to run concurrently.

[12] http://sonnyzulhuda.wordpress.com/2010/08/24/penal-code-for-cyber-crime/

3) **Online Fraud: "Woman jailed for online scam" (The Star, 24/3/2009)**

A foreign woman was jailed for a year and three months for attempting to cheat a government officer through e-mail saying he had won a "Microsoft 2008 Anniversary" lucky draw prize of US$1mil (RM3.64mil).

Peace Okotie, 26, a business student at a private college in KL, who changed her plea to guilty after a witness testified at her trial earlier, was also slapped with four months' jail for overstaying in Malaysia after her student pass expired on July 22, 2008.

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

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

Crime is a challenge for the good thinking world. While changing the time and invention of new and advanced technologies, the world of crime is also being changed. The tools and techniques are changing everyday. The burning reflection of that is, 20th centuries most important, remarkable and epoch-making invention computer related crimes, which is better known as cyber crime or cyberspace crime or simply computer crime. Now let's discuss about some of the most common and frequently committed acts wherein the computer is a tool for unlawful acts. This kind of activity usually involves a modification of a conventional crime by using computers[14] such as:

- **Financial crimes**

  This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

- **Pornography**

  This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

- **Sale of illegal articles**

  This would include sale of narcotics, weapons and wildlife etc. by posting information on websites, auction websites and bulletin boards or 167 simply

[13] http://hubpages.com/hub/Cyber-Crime
[14] http://www.cavency.com/cybercrime.html

by using e-mail communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

- **Online gambling**

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

- **Intellectual Property crimes**

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

  A counterfeit product is basically a forged electronic document prepared for the purpose of cheating and it is also sold to the public as genuine, hence the counterfeiters are punishable under Sections 468 and 471 IPC. There are many pirate websites on internet which make software available for free download or in exchange for uploaded programs. There are also many online auction sites which offer counterfeit or infringing copyright software. The webmasters of these websites are punishable under Section 120B IPC r/w Sec 63 of Copyright Act as they are part of the conspiracy by way of abetting copyright violations and enabling people to gain access to copyrighted software.

  All such people are committing offences under Section 66 of Information Technology Act, 2000 and are therefore punishable under Section 66(2) of the Information Technology Act.

- **E-mail spoofing**

  A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. E-mail spoofing can also cause monetary damage.

- **Forgery**

  Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers and high quality scanners and printers.

- **Cyber Defamation**

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

- **Cyber stalking**

  Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with e-mails etc.

- **E-mail bombing**

  This is refers to sending a large number of e-mails, to the victim resulting in the victim's e-mail account or mail servers crashing.

- **Logic bombs**

  There 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.

- **Trojan attacks**

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

- **Salami attacks**

  These attacks are used for the commission of financial crimes. The key here is to make the alternation so insignificant that in a single case it would go completely unnoticed.

- **Web jacking**

  This offence involves the taking over of control of another person's website for the purpose of causing monetary or other loss.

- **Cyber terrorism**

  Cyber terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer Virii.

- **Cyber vandalism**

  Vandalism is destroying or defacing the property of others or public property. Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals[15].

- **Pyramid schemes on the Internet**

  A pyramid scheme is a non-sustainable business model that involves promising participants payment, services or ideals, primarily for enrolling other people into the scheme or training them to take part, rather than supplying any real investment or sale of products or services to the public. Pyramid schemes are a form of fraud[16].

- **Fraud and Cheating**

  Fraud, as the intentional use of deceit, a trick or some dishonest means to deprive another of his/her/its money, property or a legal right[17].

  Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs etc.

---

[15] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

[16] http://en.wikipedia.org/wiki/Pyramid_scheme

[17] http://wiki.answers.com/Q/How_is_cheating_and_fraud_different_in_law_in_meaning

- **Information Technology Act and Indian Penal Code**

[18]Any offence under law in which an electronic document is involved can be termed generally as a "Cyber Crime". Such an electronic document can be a tool of Crime or an object of Crime.

The crime can be an "Internet Crime" where a website or an e-mail might be used as a tool or a crime involving a LAN or even a single computer. A Crime using a Mobile or ATM is also generally covered under the term "Cyber Crime" since electronic documents are involved.

Out of the crimes some crimes come under Information Technology Act 2000 and some may come under other statutes such as IPC, e.g. A defamatory/ threatening message sent through e-mail or SMS is an offence under IPC and also under amended ITA 2000. If the message is "Obscene" it may be an offence under Section 67 of ITA 2000.

A Fraud committed using web or e-mail such as the Nigerian Fraud or a Lottery fraud is an offence under IPC and not under ITA 2000.

Any offence in which an Electronic Document is accessed or altered causing a wrongful harm to some body may be an offence under Section 66 of ITA 2000.

Owing to Section 91 of the Information Technology Act, 2000, all offences under the Indian Penal Code are also applicable to acts of such nature on the internet or computer.

[19]There has never been a set in stone definition of cybercrime. The easiest way to describe cybercrime that it is any illegal activity done through the internet or on the computer.

Cybercrime can take numerous profiles and can take place nearly anywhere or anytime just like conventional crime. Criminals committing cybercrime employ numerous techniques, depending on their knowledge and their target. This should not be unexpected since cybercrime, in any case, is simply "crime" with some sort of "computer" feature.

The word cybercrime is usually limited to describing illegal activity in which the network or computer is a crucial part of the crime. However, this word additionally is used to include conventional crimes in which networks or computers are used to enable the illegal activity.

2.9 TWO TYPES OF CYBER CRIME

- **Type I** cybercrime is usually a single occurrence from the standpoint of the injured party. As an example, a person inadvertently downloads a Trojan horse which sets up a keystroke logger on their computer. On the other hand, the victim may receive an e-mail with what alleges to be a link to a recognized article, but in truth is a link to a hostile website. It is usually made possible by crime ware programs such as Virii, Trojan horses, keystroke loggers or root kits.

  Software vulnerabilities or defects frequently make available the traction for the aggressor. As an example, criminals calculating a website may seize benefit of vulnerability in a web browser to place a Trojan horse on the injured party's computer.

  Theft or exploitation of services or data by Virii or hacking, phishing, bank or

[18] http://www.ccc-rac.in/cybercrime.htm

ecommerce scam or identity theft are some, but not inclusive of this sort of cybercrime.

- **Type II** cybercrime, on the other hand, consists of, but is not restricted to actions such as extortion, stock market exploitation, cyber stalking and harassment, intricate corporate spying, child predation, blackmail and scheduling or execution of terrorist actions.

- **Type II** characteristics are:

  Type II cybercrime normally is a series of continuing actions with the objective. As an example, a person gets contacted in a chat room by another person, who, after a while, tries to create a connection. Ultimately, the criminal takes advantage of the relationship to commit an illegal offense. Another example, affiliates of a terrorist group or criminal association may use concealed communications to converse in a public forum to plan actions or talk about money laundering settings. This is usually made possible by programs that don't fit in the categorization crime ware. As an example, dialogues might use instant messaging (IM) services or data might be transmitted using FTP.

  All cyber crimes do not come under the IT Act, but many cyber crimes come under the Indian Penal Code. For example,

  a) Sending threatening messages by e-mail – Section 506 IPC & Sec 503 IPC

  b) Sending defamatory messages by e-mail – Section 499 IPC

  c) Forgery of electronic records – Section 465 IPC

  d) Bogus websites, cyber frauds – Section 420 IPC

  e) Forgery of electronic records Sec 463, 470, 471 IPC

  f) E-mail spoofing- Sec 416, 417, 463 IPC, Section 465, 419 IPC

  g) Criminal breach of trust/Fraud – Sec. 405,406,408,409 IPC

  h) Destruction of electronic evidence – Sec.204, 477 IPC

  i) False electronic evidence – Sec.193 IPC

  j) Offences by or against public servant-Sec.167, 172,173,175 IPC

  k) Web-jacking – Section 383 IPC

  l) Hacking – Section 66 IT Act

  m) Pornography – Section 67 IT Act

  n) E-mail bombing – Section 66 IT Act

  o) Denial of Service attacks – Section 43 IT Act

  p) Virus attacks – Section 43, 66 IT Act

  q) Salami attacks – Section 66 IT Act

  r) Logic bombs – Section 43, 66 IT Act

2.10 CYBER CRIME AND VARIOUS SCENARIOS

There are the various scenarios regarding numerous cyber crimes. There are cases where social networking sites are made the preferred platforms for launching attacks on the reputation of the target person. E-mail accounts are routinely hacked for

the purposes of causing monetary and data loss. Credit cards and banking information are targeted for causing wrongful loss to others. Online share trading is targeted on computer networks. Money launderers use Internet for the purpose of implementing their illegal designs.

Original software source codes, as also confidential information are made the target of theft. Piracy, whether of software or of music, continue to grow on the Internet. E-mail scams, phishing and other innovative forms of duping continue unabated on the Internet. Cyber attacks, hackings and cyber terrorism continue to be of increasing importance, as time passes by.

2.11 SOME INDIAN CASE STUDIES

1) **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.

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.

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. 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."

2) **Sony.sambandh.com Case**[20]

India saw its first cybercrime conviction in this case. 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.

[20] http://cyber-law-web.blogspot.com/2009/07/case-study-cyber-law-sonysambandhcom.html

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 Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000.

3) **Nasscom vs. Ajay Sood & Others**[21]

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. The 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 High Court stated that even though there is no specific legislation in India to penalize 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.

---

[21] http://www.e2-labs.com/49.html

The high court recognised the trademark rights of the plaintiff and passed an ex-parte adinterim 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.

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 Intellectual Propoerty 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 Intellectual Property rights.

4) **Koshy vs. State of Kerala** 2010(1) KLT945 the Kerala High Court held as follows:

3) In the Bail Application, the offences under Sections 419 and 420 of the Indian Penal Code were not mentioned. When the Bail Application came up for admission, the undertaking made by the learned Public Prosecutor appearing for respondents 1 and 3 that the petitioners will not be arrested for a period of two weeks was recorded and urgent notice was ordered to respondent No. 2, the S.I. Of Police, Rajpura City Police Station, Patiala, Punjab. It is brought to my notice that the offence under Sections 65 and 66 of the Information Technology Act is bailable in view of Section 77B of the Information Technology Act. Section 77B was introduced by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009). Section 77B provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

5) **Abhijith R. Prasad vs. State of Kerala' Represented and the Circle Inspector of Police** Bail Appl. No. 3326 of 2010 MANU/KE/0423/2010 the Kerla HC held as follows:

6) Learned Public Prosecutor submitted that the petitioner appeared before the Investigating Officer and he was interrogated. His statement was also recorded. Recovery of the relevant materials are already effected. It is also conceded that de facto complainant and the petitioner's father are on inimical terms with each other. It is also pointed out by learned Public Prosecutor that the only offence alleged against the petitioner is under Section 67 of the Information Technology Act and on first conviction, the punishment is only upto 3 years and also fine. It is further pointed out that as per Section 77B of the said Act, the offence punishable upto 3 years is only bailable.

7) On hearing both sides, I find that the petitioner has a strong and arguable case in respect of involvement of offence under Section 67 of Information Technology Act. Considering the various facts and circumstances, including the fact that recovery is already effected, I find that anticipatory bail can be granted to the petitioner on conditions. Hence, the following order is passed:

1) Petitioner shall surrender before the Magistrate Court concerned within 7 days from today.

2) On such surrender, he shall be released on bail on his executing a bond for Rs. 10,000/- with two solvent sureties each for the like sum to the satisfaction of the learned Magistrate, on the following conditions:

i) Petitioner shall report before the Investigating Officer as and when directed and co-operate with the investigation.

ii) In case, the petitioner is involved in other similar act as alleged, bail is liable to be cancelled.

6) **Avnish Bajaj vs. State (N.C.T.) of Delhi** (2005)3CompLJ364(Del), 116(2005)DLT427, 2005(79)DRJ576 the Delhi HC held as follows:

5) Sections 292 and 294 of the Indian Penal Code have also been mentioned which contemplate the selling, letting on hire, distribution or public exhibition of obscene matter. He has emphasized that the provision does not bring within its sweep the causing of the transmission in contradistinction to the publication of obscene material. Prima facie it has not been established from the evidence that has been gathered till date that any publication took place by the accused, directly or indirectly. The actual obscene recording/clip cannot be viewed on the portal of Baaze.com. This question will have to be decided. It has been argued on behalf of the accused that on coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend. Prima facie Baaze.com has endeavored to plug the loophole although it is to be expected that similarly placed persons should do so with immediate alacrity. This case will indubitably bring to the fore the dangers endemic in this business, which must be addressed forthwith.

7) Learned Counsel for the accused relies on Gurcharan Singh and Ors. vs. State (Delhi Administration), AIR 1978 SC 179. The normal rule is that ordinarily bail should be granted and its refusal should not act as a substitute for punishment.

9) The accused is enlarged on bail subject to furnishing two sureties in the sum of Rs. 1,00,000/- each to the satisfaction of the concerned Court/ Metropolitan Magistrate/Duty Magistrate. The accused shall also not leave the territories of India without the leave of the Court and for this purpose shall surrender his passport to the Magistrate. It is implicit in the grant of bail that he shall participate and assist in the investigation.

7) **Smt. Veena Verma vs. State of U.P. and Anr.** Criminal Misc. Bail Cancellation Application No. 18501 of 2009 MANU/UP/1423/2010 the Allahabad HC held as under:

9) Here in this case before this Court, it is very much relevant to note that the accused is found involved in a series of crime with the applicant even after the day he was enlarged on bail in Case Crime No. 04 of 2009 for the offence under Sections 386, 511, 506 and 509 I.P.C and Section 67 Information Technology Act. Earlier too, the accused was found involved in two criminal cases committing the crime with the applicant. After getting bail in case Crime No. 04 of 2009 on 5.6.2009 the accused continuously is found involved thereafter too in three cases registered at Case Crime No. 267 of 2009, case Crime No. 1517 of 2009 and Case crime No. 2692 of 2009 which shows that the accused has misused the liberty enlarged to him for remaining on bail thereby committing the offence regularly, harassing the complainant who is witness against him. Though I do find merely it too it sufficient ground for cancellation of the bail of the accused but one more fact too for cancellation of bail is available on record as the accused has been charge sheeted for the offence under Section 376 I.P.C too in the same case crime number, in which he was enlarged on bail merely for the offence under Sections 386,511, 506 and 509 I.P.C and Section 67 Information Technology Act. The impugned bail order can not be extended for the accused to remain on the bail as subsequently the heinous offence is found committed by him in the same case crime and the charge sheet has been submitted. Therefore, this bail cancellation

application deserves to be allowed. Hence the bail order dated 5.6.2009 passed in Bail Application No. 1212 of 2009 thereby enlarging bail to accused Sanjay Chaudhary in case crime No. 04 of 2009, under Sections 386, 511, 506 and 509 I.P.C and Section 67 Information Technology Act is hereby cancelled.

8) **Syed Asifuddin and Ors. vs. The State of Andhra Pradesh and Anr.** 2006(1) ALD (Cri) 96, 2005CriLJ4314 the AP High Court held as follows:

28) Therefore, reading Section 2(o), (ffc) and Sections 13 and 14 together, it becomes clear that a computer programme is by very definition original literary work and, therefore, the law protects such copyright. Under Section 63 of the Copyright Act, any infringement of the copyright in a computer programme/ source code is punishable. Therefore, prima facie, if a person alters computer programme of another person or another computer company, the same would be infringement of the copyright. Again the entire issue in this regard is subject to the evidence that may be led by the complainant at the time of trial. This Court, however, examined the submission of the learned senior counsel for the petitioners in the background of the provisions of the Copyright Act and observations made herein are not intended to decide the question one way or the other. The trial Court has to deal with these aspects.

29) As noticed hereinabove, unless and until investigation by the Police into a complaint is shown to be illegal or would result in miscarriage of justice, ordinarily the criminal investigation cannot be quashed. This principle is well settled and is not necessary to burden this judgment with the precedents except making a reference to R.P. Kapoor vs. State of Punjab, MANU/SC/0086/1960 : 1960CriLJ1239 ; State of Haryana vs. Bhajan Lal, 1992 Cri LJ 527 (SC) (supra) and State of Tamil Nadu vs. Thirukkural Permal, MANU/SC/0615/ 1995 : [1995]1SCR712 30. In the result, for the above reasons, Crime No. 20 of 2003 insofar as it is under Sections 409, 420 and 120B of Indian Penal Code, 1860 is quashed and insofar as the crimes under Section 65 of the Information Technology Act, 2000 and Section 63 of the Copyright Act, 1957, the criminal petitions are dismissed. The C.I.D. Police, which registered Crime No. 20 of 2003, is directed to complete investigation and file a final report before the Metropolitan Magistrate competent to take cognizance of the case within a period of three months from the date of receipt of this order.

9) **Bhim Sen Garg vs. State of Rajasthan and Ors.** 2006CriLJ3643, RLW2006(3)Raj2411, the Rajsthan High Court held as follows:

Facts:

In this case the writ petition the petitioner prayed for a writ of mandamus for quashment of FIR No. 21/2006 dated 27.01.2006 registered at Police Station Transport Nagar, Jaipur for the offences punishable under Sections 465, 469, 471, 120B, IPC and Section 65 of Information Technology Act 2000.

The Rajasthan High Court held as under:

61) Thus, in view of the test laid down by Hon'ble the Supreme Court in the case Bhajan Lai and as observed here in above, the impugned FIR No. 21/ 2006 cannot said to be false at its face value and the petitioner also not able to prove the malice against the Minister concerned and police officials.

62) In view of the observations made here in above, the present petitioner is not the rarest of rarest case which requires any interference while exercising extraordinary power under Article 226 of Constitution of India.

63) Thus, no interference whatsoever is required in the impugned FIR No. 21/ 2006 dated 27.01.2006 and the petitioner has utterly failed to make out any case that the FIR in question is false at its face value.

10) **Maqbool Fida Husain vs. Raj Kumar Pandey** 2008CriLJ4107

Facts:The present petitions seeking to challenge the summoning orders against the petitioner arise from such a contemporary painting celebrating nudity made by an accomplished painter/petitioner. The said painting depicts India in an abstract and graphical representation of a woman in nude with her hair flowing in the form of Himalayas displaying her agony. It is stated that the said painting was sold to a private collector in the year 2004 and that the petitioner did not deal with the same in any manner whatsoever after sale. Subsequently in the year 2006, the said painting entitled "Bharat Mata" was advertised as part of an on-line auction for charity for Kashmir earthquake victims organized by a non-governmental organisation with which the petitioner claims to have no involvement. It is stated that the petitioner at no point in time had given a title to the said painting. The advertisement of the said painting led to large scale protests for which the petitioner also had to tender an apology.

It is in this background that there were private complaints filed at various parts of the country being Pandharpur, Maharashtra; Rajkot, Gujarat; Indore and Bhopal, Madhya Pradesh alleging various offences against the petitioner on account of the aforesaid painting consequent whereto summons and warrants of arrest were issued against the petitioner. The petitioner approached the Supreme Court seeking consolidation of the matter. The Supreme Court acceded to the request and in pursuance to the directions passed vide order dated 04-12-2006, the said complaint cases pending consideration were consolidated and transferred to the court of the Ld. ACMM, Delhi by way of transfer petitions filed by the petitioner being T.P. (Cri.) No. 129/2006, T.P. (Cri.) No. 182/2006 and T.P. (Cri.) No. 224/2006. The Ld. ACMM, Delhi issued summons to the petitioner for various offences Under Section 292/294/298 of the Indian Penal Code ('IPC' for short) against which the present revision petitions have been filed.

The Supreme Court held as follows:

33) Thus Section 67 is the first statutory provisions dealing with obscenity on the Internet. It must be noted that the both under the Indian Penal Code, 1860 and the Information Technology Act, 2000 the test to determine obscenity is similar. therefore, it is necessary to understand the broad parameters of the law laid down by the courts in India, in order to determine "obscenity".

129) In my considered view, this particular aspect of jurisdiction fettered within the parameters of scrutiny of Section 202 of the said Code as discussed above derives its importance especially with the advent of the technological explosion where a person sitting anywhere across the globe can get access to what ever information he has been looking for just with a click of a mouse. therefore, it has become imperative that in this information age, jurisdiction be more circumscribed so that an artist like in the present case is not made to run from pillar to post facing proceedings. It was found necessary to at least examine this aspect in view of the large number of incidents of such complaints which had been brought to light by press resulting in artists and other creative persons being made to run across the length and breath of the country to defend themselves against criminal proceedings initiated by oversensitive or motivated persons including for publicity. This however is not an aspect where a direction can be issued since it is within the domain of appropriate legislation. The learned ASG while assisting this Court fairly stated that he would advice the Government to take steps by way of appropriate legislative amendments as may be proper keeping in mind the balancing of interest between the person aggrieved and the accused so as to prevent harassment of artists, sculptors, authors, filmmakers etc. in different creative fields. I say nothing more but

hope that this aspect would get the attention it deserves and the legislature in its wisdom would examine the feasibility of possible changes in law.

130) A liberal tolerance of a different point of view causes no damage. It means only a greater self restraint. Diversity in expression of views whether in writings, paintings or visual media encourages debate. A debate should never be shut out. 'I am right' does not necessarily imply 'You are wrong'. Our culture breeds tolerance- both in thought and in actions. I have penned down this judgment with this favorent hope that it is a prologue to a broader thinking and greater tolerance for the creative field. A painter at 90 deserves to be in his home – painting his canvass.

11) **Fatima Riswana vs. State Rep. by A.C.P., Chennai and Ors.** AIR2005SC712 **(Transfer of case)**

Facts:

3) The appellant is a prosecution witness in S.C. No. 9 of 2004 wherein respondents 2 to 6 are the accused facing trial for offences punishable under Section 67 of Information Technology Act, 2000 r/w Section 6 of Indecent Representation of Women (Prohibition) Act, 1986, Under Section 5 & 6 of Immoral Traffic (Prevention) Act, 1956, Under Section 27 of Arms Act, 1959 and Sections 120(B), 506(ii), 366, 306 & 376 I.P.C. The said trial relates to exploitation of certain men and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The said sessions trial came to be allotted to the V Fast Track Court, Chennai which is presided over by a lady Judge. That court also happened to be the "Mahila Courts" constituted vide Government Notification G.O.Ms. No. 556 Home (Courts II) Department of the Tamil Nadu Government, constituted to exclusively deal with offences against women and for speedy trial of cases of offences committed against women and also case under other Social Laws enacted by the Central and the State Governments for the protection of women.

The Supreme Court held as follows:

14) that the High Court has considered only the embarrassment that may be caused to the lawyers and Judges and has failed to take into consider the embarrassment that may be caused to the lady witnesses like the appellant herein who have been summoned in this case to appear before a court presided over by a male Judge to give evidence more where their own acts are part of the prosecution evidence. Therefore, if at all, there was a question of avoiding the embarrassment caused to any of the people involved in the case, in our opinion, the court ought to have considered the embarrassment that would be caused to the witness who are actually in the nature of victims while giving evidence of their acts before a male Judge. The learned counsel for the appellant, in our view, was justified in this context in relying upon the judgment of this court in the case of *State of Punjab* vs. *Gurmit Singh (supra).*

16) For the reasons stated above, we are of the considered opinion that this appeal has to be allowed in the sessions case No. 9 of 2004 now transferred to the IV Fast Track Court Chennai be transferred back to the V Fast Track Court, Chennai and the trial be proceeded before the said Fast Track Court, as expeditiously as possible keeping in mind the direction issued by the High Court in this regard.

12) **State of Punjab and Ors. vs. Amritsar Beverages Ltd. and Ors.** AIR2006SC2820, 2006(7) SCALE587, (2006)607SCC7, [2006]147STC657 (SC), 2006(2) UJ1111 (SC), the Supreme court held as follows:

7) Internet and other information technologies brought with them the issues which were not foreseen by law as for example, problems in determining statutory liabilities. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or did not have the sufficient insight to tackle with the new situation. Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus. Information Technology Act, 2000 although was amended to include various kinds of cyber crimes and the punishments therefore, does not deal with all problems which are faced by the officers enforcing the said Act.

8) We may notice some recent amendments in this behalf Section 464 of the Indian Penal Code deals with the inclusion of the digital signatures. Sections 29, 167, 172, 192 and 463 of the Indian Penal Code have been amended to include electronics documents within the definition of 'documents'. Section 63 of the Evidence Act has been amended to include admissibility of computer outputs in the media, paper, optical or magnetic form. Section 73A prescribes procedures for verification of digital signatures. Sections 85A and 85B of the Evidence Act raise a presumption as regards electronic contracts, electronic records, digital signature certificates and electronic messages.

The aforesaid cases are some of the important case studies on this subject.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain the difference between conventional crimes and cyber crimes.

.....

.....

.....

.....

.....

.....

2) Explain the reasons for cyber crimes.

.....

.....

.....

.....

.....

.....

2.12 LET US SUM UP

Thus unit deals with the conventional crimes happened through computer. It is essential to know the relation of conventional crimes with the cyber crimes. Although such crimes are required to be controlled and prevented in order to have proper utilization of cyber space in the growth and development work.

2.13 CHECK YOUR PROGRESS: THE KEY

Check your Progress 1

1) Cyber Crime is any crime that involves computer or computer system either as a target or as a medium. With this definition, one could/should not be mistaken into thinking that cyber crime only takes place when a computer genius manages to interfere with a networked computer system, bypassing complicated security, encryption or any access-controlling mechanism.

   Cyber crime includes those 'conventional crimes' in which the criminal has found a new way to launch their wrong-doing, by way of computer network or otherwise being facilitated by information technologies. The legal role of addressing and curbing cyber crime can therefore be attributed to the conventional law of crime.

2) Refer to Section 2.7

UNIT 3 CRIMES AND TORTS COMMITTED ON A COMPUTER NETWORK

Structure

3.0 INTRODUCTION

With the recent advances in computer technology, many companies have become increasingly dependent on the Internet and other computer-related technologies to manage their businesses and sell their products. Many companies find that they need to operate in cyberspace to meet the demands of their customers and compete with their competitors. Whatever the reason, these new technologies implicate new

risks and liabilities for businesses. Among these risks is the potential that activities in cyberspace may give rise to tort claims, often called "cybertorts." With the ubiquity of the Internet, even small U.S.-based companies with a minimal presence in cyberspace may find that their activities nonetheless expose them to liability in foreign jurisdictions with different standards of behaviour. Furthermore, companies may find that their traditional insurance policies do not cover these cybertorts especially when a lawsuit is brought outside the United States[1].

The increasing use of Information Technology (IT), however, brings with it new challenges and threats. Amongst the most significant is the security threat, including data theft, piracy, hacking, identity theft, violation of intellectual property rights etc.[2]

3.1 OBJECTIVES

After going through this Unit, you should be able to:

- explain different types of cyber tort;
- understand tortious liability in cyber crimes;
- understand tort liability for creators of fake profiles on social networking websites;
- explain liability of service providers in tort;
- find out cyber tort in USA, France and Australia; and
- understand legal issues relating to Wikileaks.

3.2 MEANING AND DEFINITION OF TORT[3]

The term tort is the French equivalent of the English word 'wrong' and of the Roman law term 'delict'. The word tort is derived from the Latin word tortum which means twisted or crooked or wrong. As a technical term of English law, tort has acquired a special meaning as a species of civil injury or wrong. It was introduced into the English law by the Norman jurists.

In general terms, a tort may be defined as a civil wrong independent of contract for which the appropriate remedy is an action for unliquidated damages.

According to Salmond – A tort is a civil wrong for which the remedy is a common action for unliquidated damages and which is not exclusively the breach of a contract or the breach of a trust or other mere equitable obligation.

According to Winfield – Tortuous liability arises from the breach of a duty primarily fixed by law; this duty is towards persons generally and its breach is redressible by an action for unliquidated damages.

A tort is a civil, legal injury to a person or property caused by a breach of a legal duty. Plaintiff (the injured party) sues the Defendant (the Tortfeasor) for damages.

Three kinds of Torts:
i) Intentional
ii) Unintentional (negligence-no fault)
iii) Strict Liability

[1] http://www.law.duke.edu/journals/dltr/articles/2001dltr0023.html
[2] http://www.hg.org/article.as/pid=5260.htm
[3] http://legalservicesindia.com/article/article/fundamental-liability-theory-460-1.html

1) **Intentional Torts against Persons**

- Assault and Battery
- Assault: the reasonable apprehension or fear of immediate contact
- Battery: completion (contact) of the assault

Defenses

- Consent
- Self-Defense and Others
- Defense of Property

2) **Unintentional Torts against Persons**

- False Imprisonment
- Confinement or restraint of another person's activities without justification
- Merchants can detain a suspected shoplifter as long as there is probable cause
- Infliction of Emotional Distress
- Extreme and outrageous conduct

Defamation: Publication of a false statement (oral or written) that injures a person's good reputation.

Publication: third party must hear or see statement. Statements made on the internet may be actionable. An individual who re-publishes the statement will be liable. Statement must hold someone up to contempt, ridicule or hatred in the community Slander per se (no proof of damages is required)

Defenses

- Truth is normally an absolute defense.
- Statement was Privileged.
- Absolute: judicial and legislative proceedings.
- Qualified: good faith, limited.
- Public Figures: plaintiff must show statement made with "actual malice."
- Invasion of the Right to Privacy.
- Person has the right to solitude. Breach of that duty is a tort.
- Appropriation.
- False light.
- Public Disclosure of Private Facts.
- Rights of Internet users.
- Misrepresentation (Fraud): Intentionally deceive another to believe in a condition that is different from the condition that already exists.
- Knowing misrepresentation of fact.
- Intent to induce innocent party to rely.

- Justifiable reliance by innocent party.
- Causation and Damages.
- Contrast: "puffery" or statements.
- Wrongful Interference with Contracts.
- Valid, enforceable contract exists between two parties.
- Third party knows about contract.
- Third party intentionally causes either party to breach the original contract.
- Wrongful Interference with Business Relationship.
- Distinguish competition vs. predatory behavior: Predatory behavior is unlawfully driving competitors out of market. To prevail, Plaintiff must show Defendant targeted only Plaintiff's customers and product.
- Defenses to Wrongful Interference.
- Interference was justified or permissible.
- Trespass to Land.

Trespass to Personal Property

- Conversion
- Disparagement of Property
- Slander of Quality
- Slander of Title

The Nature of Tort[4]

Our first difficulty in tackling law of torts is to ascertain the contents and boundaries and limits of the subject. Assault, libel and deceit are torts. Trespass to land and wrongful dealing with goods by trespass, "conversion," or otherwise are torts. The creation of a nuisance to the special prejudice of any person is a tort. Causing harm by negligence is a tort. So is, in certain cases, the mere failure to prevent accidental harm arising from a state of things which one has brought about for one's own purposes. Default or miscarriage in certain occupations of a public nature is likewise a tort, although the same facts may constitute a breach of contract and may, at the option of the aggrieved party, be treated as such.

3.2.1 Tort and Crime[5]

A crime is a wrong committed against state: it is not necessarily against a private right. The state can punish people for criminal acts through measures that range from money penalties or fines to imprisonment. Private Citizens can also bring legal action for crimes, but rarely do so.

Torts or Civil wrongs are wrongs committed against private entities such as companies or private citizens, but are not necessarily offences against the state. The courts can remedy a tort by ordering the liable party to correct the wrong, discontinue an act or pay compensation or indemnity.

[4] http://legalservicesindia.com/article/article/fundamental-liability-theory-460-1.html
[5] http://legalservicesindia.com/article/article/fundamental-liability-theory-460-1.html

3.2.2 General Element in Torts

The main objectives of the law of tort are to protect harms to the properties, body and prestige of the persons. Being in that essence there are the basic principles in tort that were established, following are the principles itself:

1) **Act or Omission**

To constitute a tort there must be a wrongful act, whether of omission or commission, but not such acts as are beyond human control and as are entertained only in thoughts. An omission is generally not actionable but it is so exceptionally. Where there is a duty to act an omission may create liability. A failure to rescue a drowning child is not actionable, but it is so where the child is one's own. A person who voluntarily commences rescue cannot leave it half the way. A person may be under duty to control natural happenings to his own land so as to prevent them from encroaching others' land.

2) **Voluntary and Involuntary Acts**

A voluntary act has to be distinguished from an involuntary act because the former may involve liability and the latter may not. A self willed act like an encroachment for business, is voluntary, but an encroachment for survival may be involuntary. The wrongfulness of the act and the liability for it depends upon legal appreciation of the surrounding circumstances.

3) **Malice**

Malice is not essential to the maintenance of an action for tort. It is of two kinds, 'express malice' (or malice in fact or actual malice) and 'malice in law' (or implied malice). The first is what is called malice in common acceptance and means ill will against a person; the second means a wrongful act done intentionally without just cause or excuse.

4) **Intention, Motive, Negligence and Recklessness**

The obligation to make reparation for damage caused by a wrongful act arises from the fault and not from the intention. Any invasion of the civil rights of another person is in itself a legal wrong, carrying with it liability to repair it necessary or natural consequences, in so far as these are injurious to the person whose right is infringed, whether the motive which prompted it be good, bad or indifferent. A thing which is not a legal injury or wrong is not made actionable by being done with a bad intent. It is no defence to an action in tort for the wrong doer to plead that he did not intend to cause damage, if damage has resulted owing to an act or omission on his part which is actively or passively the effect of his volition. A want of knowledge of the illegality of his act or omission affords no excuse, except where fraud or malice is the essence of that act or omission. For every man is presumed to intend and to know the natural and ordinary consequences of his acts. This presumption is not rebutted merely by proof that he did not think of the consequences or hoped or expected that they would not follow. The defendant will be liable for the natural and necessary consequences of his act, whether he in fact contemplated them or not.

5) **Malfeasance, Misfeasance and Non-Feasance**

The term 'malfeasance' applies to the commission of an unlawful act. It is generally applicable to those unlawful acts, such as trespass, which are actionable per se and do not require proof of negligence or malice. The term 'misfeasance ' is applicable to improper performance of some lawful

act. The term 'non-feasance' applies to the failure or omission to perform some act which there is an obligation to perform.

6) **Fault**

Liability for tort generally depends upon something done by a man which can be regarded as a fault for the reason that it violates another man's right. But liability may also arise without fault. Such liability is known as absolute or strict liability.

3.2.3 Intention and Tortuous

Liability

According to an interpretation intention is a single mental state that cannot be assimilated or reduced to predictability and as such it deserves special treatment by law

- Intention as a mental condition that involves a plan to take a degree in the future
- Intention as a mental condition that involves the desire for a certain state of things

The two notions of intent leads to different results: the first sense focuses on planning while the latter focuses on a desire to achieve a result, even if that state of mind was formed immediately.

Elements of Intentional Tort

There are certain elements which are prerequisite for invoking liability of tortuous nature in case of intention giving rise to tort. These are:

Voluntary act – there must be a self willed action that forms a major element in intentional tort.

Mental state – mental element in divided in two sub parts, fulfilling which a liability arises in tort. They are purposeful and knowing.

Motive – Motive is also referred as purposeful which can be conscious desire to achieve the result.

Malice – malice is also referred as knowing which is bad intention to do something and actual knowledge to a substantial certainty that the result will occur.

Examples of Intentional Tort: Assault, Battery, Trespass to land and Trespass to chattels, False Imprisonment, Intentional Infliction of Emotional Distress and conversance.

Strict Liability – In law, strict liability is a standard for liability which may exist in either a criminal or civil context. A rule specifying strict liability makes a person legally responsible for the damage and loss caused by his or her acts or omissions regardless of culpability

In tort law, strict liability is the imposition of liability on a party without finding a fault. The plaintiff only needs to proof that the tort occurred and that the defendant was responsible. Strict liability is imposed for legal infractions and that are neither good faith nor the fact that the defendant took all possible precautions are valid defences. It often implies to those engaged in hazardous or inherently dangerous ventures. The law includes strict liability to situations it considers to be inherently dangerous. It discourages reckless behaviour and needless loss by forcing potential defendants to take every possible precaution.

Absolute Liability – This has come from modern law of tort which means liability without fault, i.e. liability without intention or negligence. Liability of this kind is exceptional under common law as the ordinary rule is that a person is only liable for harm due to his intention or negligence and not for other kind of harm which would be merely an inevitable accident.

All the aforesaid principles relating to the law of torts, wherever relevant, are fully applicable in the context of cyber torts.

3.3 CYBER CRIMES AND TORT

The Law of Crime generally emphasizes more upon corporal punishment whereas the law of tort emphasizes the monetary compensation. The gravity and the character of commission of Cyber wrong or offence have to be considered minutely to designate as tort or crime.

Cyber crimes are the crimes which targets the computer database and systems. They usually 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 means 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 programmed plans, list of customers etc.), selling illegal 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 consent of the individual.

Cyber Tort is a tort committed in cyberspace[7].

Torts may be of different nature such as environmental and toxic torts, cyber torts, corporate torts, employment torts, medical malpractice torts, sports torts, product liability torts, marital torts, intentional torts, economic torts etc. Law of Torts is a developing subject; it has grown for centuries and is still growing.

Torts in the area of cyberspace and the immunity created by the court rulings and federal statutory restrictions for the torts committed in the area of cyberspace. The courts have applied the concept of personal property tort law of misappropriation of trade secrets, conversion and trespass to chattels to the torts related to cyberspace.[8]

3.3.1 Different Types of Cyber Tort

A cyber wrong or offence can be committed against person and property[9]

Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the real world. So cyber wrong or offence can be committed against persons and property in relation to the cyber space like other civil wrong or crime. It includes unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs,

[6] http://www.thedailystar.net/law/2004/08/03/campaign.htm
[7] www.jdcc.edu/includes/download.php
[8] http://www.nbcindia.com/descriptions.asp/6v6yr_vq=ELLDGFH&Book=Tortious-Liability-Emerging-Trends.htm
[9] http://www.thedailystar.net/law/2004/08/03/campaign.htm

unauthorized possession of computerized information, the transmission of pornography, harassment of a person with the use of a computer such as e-mail, cyber-stalking and spreading computer viruses as well.

Cyber Stalking – Cyber stalking occurs when a person is followed and persuaded online. In other words, their privacy is invaded. It is a form of harassment and can disrupt the life of the victim leaving them feeling afraid and threatened.

In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications. Harassment can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender. Harassment may also include threats, sexual remarks, pejorative labels (i.e. hate speech).

A particularly disturbing form of harassment is sending a forged e-mail that appears to be from the victim and contains racist remarks or other embarrassing text, that will tarnish the reputation of the victim[10].

Cyber Breach of Privacy – With the advent of multi channel televisions all over the world and fast spreading internet network, the privacy of an ordinary man is increasingly under threat. Breach of privacy is a kind of cyber tort which affects a common man.

[11]With the rise of the Internet, national variations in substantive tort law become increasingly important. The privacy rights of the individual vary significantly under different legal regimes. French law, for example, differs markedly from U.S. privacy-based torts.

"While the public activities of such persons necessarily subject more of their lives to legitimate public scrutiny, a public official or figure may shield from inquiry and intrusion those aspects of private life not related to the conduct of the public activities." Under French law, public officials and public figures may choose to protect their autonomy by withdrawing "from the public arena and return to the private domain personal information previously divulged."

In a United Kingdom case, the court ruled that sharing of personal information on an electoral register was a violation of the European Union Data Protection Directive.

In Robertson vs. Wakefield Metropolis Council, the plaintiff filed suit against his local election authority over the disclosure of personal information on the electoral registers. The United Kingdom's Highest Court held that the local governmental authority violated both the UK Data Protection Directive and the European Convention on Human Rights by disclosing personal information.

Cyber Obscenity – Cyber space offers a very wide range of pornography and makes children and women vulnerable of trafficking. This also includes child pornography and sexting and internet rape.

In Lefebure vs. Lacambre[12], a French court found an ISP liable for publishing erotic images of the plaintiff on its Web site. "Under French law, an Internet Service Provider is responsible for the morality of the content distributed via the client-operated Web sites it hosts and may be liable for violations of privacy." The French plaintiff contended that "the ISP violated her privacy and damaged her professional reputation by allowing a subscriber to publish nude photographs of her on a Web site." The French court ordered the offending Web site be shut down under the threat of a fine of 100,000 francs per day.

---

[10] http://www.rbs2.com/ccrime.htm

[11] http://www.law.suffolk.edu/faculty/add/infor/ustad04_JHTL_Lambert_RustadKoenig.pdf

[12] http://www.law.suffolk.edu/faculty/add/infor/ustad04_JHTL_Lambert_RustadKoenig.pdf

Cyber Defamation – Due to expansiveness of the internet for a, defamation is quite possible. Cyber defamation is statements that are unflattering, annoying, irksome, embarrassing or hurt one's feelings are not actionable.

[13]Defamation in cyber cyberspace is a tort that occurs when a party communicates an untrue statement in the factual form about another to a third party by e-mail or source of the World Wide Web. The information on what was said must be given by the provider of the internet service upon request by a law enforcement agency in pursuit of a warrant. When an internet service provides this information to a law enforcement agency this is not an act of invasion of privacy, but merely a means to protect society.

Unauthorized Use (tort against chattels)[14] – Unauthorized use of computers tends generally takes the following forms:

Computer voyeur-The criminal reads (or copies) confidential or proprietary information, but data is neither deleted nor changed. E.g. In 1999, the Melissa virus infected a [possibly confidential] document on a victim's computer, then automatically sent that document and copy of the virus via e-mail to other people. Subsequently, the SirCam and Klez malicious programs made a similar release of [possibly confidential] documents from a victim's computer. These malicious programs are a new way to release confidential information from a victim's computer, with the confidential information going not to the author of the malicious program, but to some person unknown to the author of the malicious program.

Changing data – For example, change a grade on a school transcript, add "money" to a checking account etc. Unauthorized changing of data is generally a fraudulent act.

Deleting data – Deleting entire files could be an act of vandalism or sabotage.

Altering websites- In recent years, there have been a large number of attacks on websites by hackers who are angry with the owner of the website. Victims of such attacks include various U.S. Government agencies, including the White House and FBI. Attacking the FBI website is like poking a lion with a stick. In a typical attack, the hacker will delete some pages or graphics, then upload new pages with the same name as the old file, so that the hacker controls the message conveyed by the site.

Denial of Service (DoS) Attacks – A denial of service attack occurs when an Internet server is flooded with a nearly continuous stream of bogus requests for webpages, thereby denying legitimate users an opportunity to download a page and also possibly crashing the webserver.

Malicious computer programs – The following are general terms for any computer program that is designed to harm its victim(s): malicious code, malicious program, malware (by analogy with "software") and rogue program Malicious computer programs are divided into the following classes:

A virus is a program that "infects" an executable file. After infection, the executable file functions in a different way than before: maybe only displaying a benign message on the monitor, maybe deleting some or all files on the user's hard drive, maybe altering data files. There are two key features of a computer virus: the ability to propagate by attaching itself to executable files (e.g. application programs, operating system, macros, scripts, boot sector of a hard disk or floppy disk etc.)

---

[13] http://www.oppapers.com/essays/Copyright-Laws-Computer-Programs-Cyberspace-Tort119316.htm

[14] http://www.rbs2.com/ccrime.htm

Running the executable file may make new copies of the virus. The virus causes harm only after it has infected an executable file and the executable file is run[15].

The first court to apply trespass to chattels to contain spam was CompuServe vs. Cyberpromotions, Inc. In that case, CompuServe filed for a preliminary injunction against Cyberpromotions, a bulk e-mailer. The CompuServe court ruled that there is no First Amendment constraint on applying the tort of trespass to chattels to enjoin spam.

In America Online, Inc. vs. LCGM widespread spamming was held to be a trespass to chattels as well as a violation of the Computer Fraud and Abuse Act and a trademark violation. In many of the U.S. spamming cases, the courts awarded damages as well as injunctive relief under causes of action based upon personal property torts.

In American Online, Inc. vs. Nat'l Health Care Disc., Inc., the court found the commercial e-mail actions to constitute trespass to chattels as well as a violation of state and federal computer abuse laws as well other causes of action. The court calculated damages by charging the spammer $2.50 per thousand messages for a total of $337,500.

3.4 ESTABLISHMENT OF TORTIOUS LIABILITY IN CYBER CRIMES

Cyber crime is a kind of crime in which generally offenders of crimes are generally hidden. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of other countries. Basic liability in cyber crime is established through the principle of neighbourhood established from the case of donoghue vs. stevenson. The major liability in cyber tort in India is through Information Technology Act, 2000 (as amended)[16].

Victim(s) of computer crimes can sue the perpetrator in tort. For example, unauthorized use of a computer system could be "trespass on chattels". A computer voyeur might also be sued in tort for invasion of privacy or disclosure of a trade secret. A harasser might be sued in tort for intentional infliction of emotional distress. There is also the possibility of a class action by corporate and personal victims against a person who wrote and initially released a computer virus.

There is another remedy in civil law, besides damages awarded in tort litigation: a victim can get a temporary restraining order (TRO), then an injunction, that enjoins continuance of wrongs (e.g. disclosure of proprietary or private data) that will cause irreparable harm or for which there is no adequate remedy at law[17].

3.5 CYBERTORTS AGAINST PROPERTY[18]

Cyber-Torts against property involve cases where personal property was involved in a cyber-crime. They involve Trespass to Personal Property and Conversion. Because online "property" is usually intangible, there was much discussion on how to define the limits and boundaries of cyber-torts. Because the law requires a physical device or object to be harmed, there were some arguments on how to bring our digital age in line with our legal system. The first Tort applied to the

[15] http://www.law.suffolk.edu/faculty/add/infor/ustad04_JHTL_Lambert_ RustadKoenig.pdf
[16] http://legalservicesindia.com/article/article/fundamental-liability-theory-460-1.html
[17] http://www.rbs2.com/ccrime.htm
[18] https://wikispaces.psu.edu/display/IST432TEAM21/Cybertorts+against+Property

digital age is Trespass to Personal Property. Trespass to Personal Property or more specifically, Trespass to Chattel has been applied to many cases in the electronic age. It has been applied to cases where bulk e-mail systems or unsolicited programs are accessing servers and slowing them down.

3.5.1 Trespass to Chattel[19]

Trespass to chattels is a tort whereby the infringing party has intentionally (or in Australia negligently) interfered with another person's lawful possession of a chattel (movable personal property). The interference can be any physical contact with the chattel in a quantifiable way or any dispossession of the chattel (whether by taking it, destroying it or barring the owner's access to it).

The antiquated common law tort of trespass to chattels has been invoked in the modern context of electronic communications to combat the proliferation of unsolicited bulk e-mail, commonly known as spam. In addition, several companies have successfully used the tort to block certain people, usually competitors, from accessing their servers. Though courts initially endorsed a broad application of this legal theory in the electronic context, more recently other jurists have narrowed its scope. As trespass to chattels is extended further to computer networks, some fear that plaintiffs are using this cause of action to quash fair competition and to deter the exercise of free speech; consequently, critics call for the limitation of the tort to instances where the plaintiff can demonstrate actual damages.

3.5.2 Rules for Trespass to Chattels

The trespass to chattels tort punishes anyone who substantially interferes with the use of another's personal property or chattels. Plaintiffs must show that the offender had intentional physical contact with the chattel and that the contact caused some substantial interference or damage. The courts that imported this common law doctrine into the digital world reasoned that electrical signals travelling across networks and through proprietary servers may constitute the contact necessary to support a trespass claim. Applying this common law action to computer networks, plaintiffs must first prove that they received some type of electronic communication (typically bulk e-mail or spam) that the defendant intentionally sent to interfere with the plaintiff's interest in his or her property and second that this communication caused a quantifiable harm to their tangible property, such as impaired functioning of the computer, network or server.

3.5.3 Conversion[20]

Another aspect of Cyber-Torts is the tort of Conversion. Conversion is a tort defined as "a voluntary act by one person inconsistent with the ownership rights of another." Conversion was initially not applicable to online issues and cyber crime because of the intangibility of electronic records. However, in 2006, in the case of Shmueli vs. Corcoran Group, the court ruled that electronic data is property just the same, even if it is intangible. The court reasoned that any electronic record could be printed or written down on paper and thus become a tangible object. "Personal papers, values and effects" were applicable to conversion and thus electronic records could be converted as well.

In Kremen vs. Cohen, the plaintiff was awarded damages because the defendant acquired the rights to the domain name www.sex.com through misrepresentation. Kremen was awarded $65 million in damages from the result of conversion. However, in the 2007 English court case of OBG Ltd. V Allan, the court ruled that

---

[19] http://en.wikipedia.org/wiki/Trespass_to_chattels#The_Backlash_Against_the_Tort.E2.80.99s_Expansion

[20] https://wikispaces.psu.edu/display/IST432TEAM21/Cybertorts+against+Property

intangible property could not be classified under the tort of conversion and could not be awarded damages.

3.5.4 Denial of Service (DoS) Attack[21]

Denial of service (DoS) attacks have emerged as a significant cyber attack weapon. A DoS attack aims to deprive legitimate users of a resource or service provided by a system, by overloading the system with a flood of data packets, thus preventing it from processing legitimate requests.

There are two main categories of denial of service attacks, namely vulnerability attacks and flooding attacks. Vulnerability attacks, as the name suggests, exploit a vulnerability in the target application.

For instance, a vulnerability known as the buffer overflow, allows an attacker to remotely inject malicious code into a target and deny service from a distance. The malicious code may, for instance, be programmed to severely slow down or crash the target, by monopolizing a significant amount of memory, bandwidth and computational power. The infamous Internet worm, W32/CodeRed, exploited a vulnerability in Microsoft's Internet Information Services (IIS) web servers and attempted to launch denial of service attacks on the official White House Web page.

A flooding attack does not exploit vulnerability, but simply overwhelms the resources of its target with a vast number of apparently legitimate messages. An attack can, of course, fall into both categories.

The success of a DoS attack involves the cooperation of a number of players. The chain consists of (1) The attackers; (2) Computer users whose machines are enlisted by the attackers and turned into zombies, (3) Target Internet sites; (4) The software vendor responsible for the exploited security vulnerabilities and (5) Network intermediaries and backbone network service providers, who deliver the attack traffic.

A case involving a DoS attack is a typical "concurrent efficient causes case." A concurrent efficient causes case is one where several defendants' wrongdoing are but-for causes of the same harm. Typically, one defendant, the original tortfeasor, is responsible for the original cause of the harm. Then, a subsequent tortfeasor intervenes and commits a second tort, which is also a but-for cause of the same harm. The last wrongdoer's liability is undisputed, but a plaintiff may be interested in suing the original tortfeasor, who may be the only solvent defendant.

3.6 LIABILITY

In a DoS attack, the actual attackers are the immediate wrongdoers, but courts may extend liability to other tortfeasors who have contributed to the attack. Vendors of vulnerable software may be held liable for facilitating DoS attacks and owners of inadequately secured zombie and target computers may be held liable for failing to take corrective precautions that could have prevented the attack. The vendor may also be held liable for exposing the victims of the attack to the inadvertent failure of the computer owners to fix the vulnerability.

Courts may also extend liability for a DoS attack to tortfeasors who intentionally failed to take a corrective precaution, such as owners of the intermediate and target computers whose failure to correct a security vulnerability was an efficient cause of the attack. And courts extend liability to tortfeasors who intentionally exposed a plaintiff to the inadvertent negligence of a third party.

[21] http://www.austlii.edu.au/au/journals/UNSWLRS/2007/3.html

A civil action involving a DoS attack would most likely be pursued under a negligence theory, the most widely used theory of tort liability. Negligence is generally defined as a breach of the duty not to impose an unreasonable risk on society. The concept of "unreasonable risk" is general and includes threats to information security, such as DoS attacks. A victim of a DoS attack may therefore bring legal action under a negligence theory against anyone who failed in a duty to reduce or eliminate a risk associated with the attack.

To pursue a successful negligence cause of action, a victim of a DoS attack has to prove (1) that the defendant had a duty to the plaintiff to take reasonable care to avoid the attack or reduce its risk, (2) that she breached that duty, (3) that the breach was the actual and legal cause of the attack and (4) that the breach resulted in actual harm.

In Lunney vs. Prodigy Services Co., the court held that the defendant, an Internet Service Provider (ISP) was not negligent for allowing an imposter to send threatening e-mail messages on a Prodigy account. The court declined, as a matter of public policy, to impose a duty on ISPs to screen all their e-mail communications, reasoning that the result would be "to open an ISP to liability for the wrongful acts of countless potential tortfeasors committed against countless potential victims."

Damages related to cyber attacks may be recoverable, the economic loss rule notwithstanding, (i) where a cyber attack, such as a DoS attack, has caused physical harm due to the malfunction of a computer system in applications such as medical systems, aviation and nuclear energy;(ii) in the few jurisdictions which have relaxed the rule against recovery for pure economic loss; and (iii) because an increasing number, perhaps a majority, of jurisdictions recognize electronic information as legally protected property. The trend towards recovery for computer-related economic loss has been recognized by United States Congress, as well as State Legislatures. The Computer Fraud and Abuse Act, for instance, allow hacking victims to recover for economic harm.

3.7 TORT LIABILITY FOR CREATORS OF FAKE PROFILES ON SOCIAL NETWORKING WEBSITES[22]

A Social Networking Service (SNS) allows users to be part of an online community with other users. SNSs have been defined as websites that that allow users to: "(1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection and (3) view and traverse their list of connections and those made by others within the system." Most SNSs also provide their users with a forum for communicating with fellow users. For example, Facebook.com lets a user write messages on another user's profile, MySpace.com provides weblogs on which its users can write and Twitter.com lets a user post short messages for others to read.

The most extreme case to date is United States vs. Drew. This case involved a 49-year-old woman who created a fake SNS profile to bully a 13-year-old girl. Lori Drew created a fake profile on MySpace pretending to be a 13-year-old boy. Drew used the profile to be friend, date and then break up with Megan Meier. Afterwards Drew continued to bully the girl until Megan committed suicide. A California jury found the defendant guilty, but the judge vacated the judgment because the statute she was convicted under was unconstitutionally vague. Although the guilty verdict

[22] http://jip.kentlaw.edu/art/Volume%201010%20Chi-Kent%203%20Intell%20 Prop%201.pdf

was vacated for procedural reasons, Drew shows that courts and juries are willing to hold people accountable for actions that take place on SNS websites.

Many victims of fake profiles do not know what legal remedies are available to address this problem. Although the law is still struggling to catch up to this recent development of fake profiles on SNSs, the courts can rely on the tools that have been a part of the American jurisprudence for many years to provide legal remedy to victims of fake profiles.

The Restatement (Second) of Torts was § 652A, which distinguished between four categories of invasion of privacy. These four categories were delineated in exactly the same way as in a famous article by Dean William Prosser.

The categories are: right of privacy, misappropriation of name or likeness, right of publicity and publicity that unreasonably places another in a false light.

The two causes of action for the tort of misappropriation of name or likeness and the tort of violation of right of publicity are similar and easily confused. This is partially because of the similarity in proof required to establish both claims. As the court in Berosini held that the distinction between these two torts is the interest each seeks to protect. The appropriation tort seeks to protect an individual's personal interest in privacy; the personal injury is measured in terms of the mental anguish that results from the appropriation of an ordinary individual's identity. The right to publicity seeks to protect the property interest that a celebrity has in his or her name.

3.7.1 Misappropriation of Name or Likeness

Misappropriation of Name or Likeness is a cause of action that protects an individual from unauthorized use of his identity. Originally this was not a separate tort but rather was a part of invasion of privacy. Dean Prosser differentiated Misappropriation from other forms of invasion of privacy in his article "Privacy." The California Court of Appeals adopted Dean Prosser's elements for establishing a misappropriation of name or likeness claim in Eastwood vs. Superior Court. These elements are:

"1) the defendant's use of the plaintiff's identity;

2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise;

3) lack of consent; and

4) resulting injury."

3.7.2 Use of Plaintiff's Identity

The defendant cannot use the plaintiff's identity. While this concept is obvious when applied to the plaintiff's name or picture, allusions to the plaintiff may be protected as well. The Minnesota district court has upheld protection for a plaintiff's pseudonym as long as it clearly identifies the plaintiff. Other courts have held that a prima facie case for misappropriation can be established if the name used clearly identifies the wronged person. In Hirsch, the defendant advertised a women's shaving gel and called it "Crazylegs." Crazy Legs is the well-known nickname for the plaintiff, former professional football player Elroy Hirsch. Although the defendant did not use Hirsch's nickname for a commercial advantage, the Wisconsin Supreme Court held the plaintiff had a property right in his identity and the plaintiff's identity includes his nickname.

3.7.3 Use must be for Defendant's Advantage

For a successful claim of misappropriation of name or likeness, the plaintiff must prove the defendant has gained in some way. When the defendant uses the plaintiff's identity to gain economically it is easy for the court to determine that this element has been satisfied. For example, in Michaels vs. Internet Entertainment Group, Inc., the defendant distributed an adult video starring musician Brett Michaels. The defendant was an Internet website that sold subscriptions to customers. The subscription service had approximately 100,000 members and its president estimated that up to one-third of the members would cancel their subscriptions if not for the video containing the plaintiff. The court determined the enticement to continue paying a monthly membership fee was enough to satisfy the advantage element of the cause of action.

Courts will still allow the plaintiff to recover under a misappropriation cause of action even if the defendant uses the plaintiff's identity for non-commercial benefit. The defendant only has to act for his own benefit even if the benefit sought is not a pecuniary one.

3.7.4 Lack of Consent

For liability in a misappropriation action, the plaintiff must prove that he did not consent to the defendant using the plaintiff's identity. Even if the plaintiff can establish that a prohibited use has occurred, the court will not allow recovery if it believes the plaintiff consented to the use of his identity. This consent can be expressly given by the plaintiff or implied from the plaintiff's actions.

3.7.5 Resulting Injury

The final element the plaintiff must establish for a claim of misappropriation of name or likeness is that the defendant's actions resulted in an injury. The plaintiff does not have to allege that a certain amount of injury occurred or make an "estimate in dollars and cents [of] the extent of plaintiff's suffering." In Kunz, the defendant took a picture of the plaintiff without her knowledge to use as an advertisement for defendant's business. The trial court dismissed the plaintiff's complaint principally because the plaintiff failed to prove any actual harm. The Kansas Supreme Court reversed the trial court's dismissal of the complaint because the showing of an injury is possible without the showing of a specific loss.

The California Appeals Court adopted Kunz by holding that any invasion of a legal right is an injury, although without proof of material harm the plaintiff may only be entitled to nominal damages. The court in Fairfield held "special damages need not be charged or proven and if the proof discloses a wrongful invasion of the right of privacy, substantial damages for mental anguish alone may be recovered." The unauthorized use of a person's name is an actionable invasion of the plaintiff's rights even if the injury was slight.

While it is necessary to show that harm resulted from the defendant's action, proving harm in a misappropriation of name action can be easy. Many states hold that as long as the plaintiff can prove an unauthorized use of his name, it is not necessary that "it be alleged or proved that such unauthorized use will damage him." In situations where a person's name was misappropriated, the court will generally presume the harm. Thus courts will generally presume harm when a person's name is misappropriated.

3.8 RIGHT OF PUBLICITY

The right of publicity is the inherent right in every person to control the commercial use of his identity. This right is generally treated as a property right that a person

has in his identity. Although many corporations have SNS profiles, a corporation generally does not have the same right to protect itself from the unauthorized use of its identity.

Thomas McCarthy determined that there are three elements that make up the prima facie case of a violation of someone's right of publicity. These elements are: a) Validity; b) Infringement; and c) Damage.

1) **Validity**

The validity element requires the plaintiff to prove that the defendant used or is using the plaintiff's identity without permission. According to McCarthy, this element is established when "either [the] plaintiff's own identity is in issue or that plaintiff is an assignee or exclusive licensee of someone else's right of publicity." Courts have characterized and protected a person's identity as his property.

The Presley's Estate court defined the right of publicity as "the right of an individual, especially a public figure or a celebrity, to control the commercial value and exploitation of his name and picture or likeness and to prevent others from unfairly appropriating this value for their commercial benefit." The court said the underlying concept was the right to control the commercial exploitation of one's name and likeness.

2) **Infringement**

To establish this element, the plaintiff must prove that the defendant used the plaintiff's identity without the plaintiff's consent. The infringement of the right of publicity is an invasion of the plaintiff's substantial property interest. This infringement can be in the plaintiff's entire act, his likeness or even his style.

Additionally, courts have held that a defendant does not need to know that its use was without the plaintiff's consent to be liable for a violation of the plaintiff's right of publicity. In Welch vs. Christmas, the court held that knowledge, malice and recklessness were not elements of a violation of someone's right of publicity.

3) **Damages**

The right of publicity protects people from losing the benefit of their work put into creating a marketable image. A person can seek a court order to protect and control the commercial value in his or her name or likeness.

The plaintiff in a violation of right of publicity action does not need to show that the defendant made money from the plaintiff's name or likeness. In Henley vs. Dillard Dept. Stores, the plaintiff was a well-known musician named Don Henley. The defendant was a department store that created a line of clothing named after the plaintiff without his consent or knowledge.

The defendant argued that plaintiff's right of publicity claim must fail because the defendant did not generate sufficient revenue to cover the costs of the advertisements. However, the court determined that the plaintiff only has to prove that defendant received a commercial benefit from use of plaintiff's name or likeness that he would not have received without the plaintiff's name or image.

Similar to the misappropriation cause of action, the Illinois Court of Appeals held that courts will presume damages if someone infringes another's right to control his identity, so claimant does not need to prove actual damages.

The court held that even if the plaintiff cannot prove actual damages from the defendant's use of the plaintiff's identity, the court would presume damages

from an unauthorized use. Since the plaintiff could not prove actual damages, the court awarded only nominal damages. However, since courts will generally presume damages from the unauthorized use of a person's identity, nominal damages are sufficient to satisfy the damage element.

3.9 LIABILITY OF SERVICE PROVIDERS IN TORT[23]

In the United States of America, ISPs and other service providers unduly restricted customers' actions for fear of being found legally liable for customers' conduct. The act was passed in part in reaction to the 1995 decision in **Stratton Oakmont, Inc. vs. Prodigy Services Co.,** which suggested that service providers who assumed an editorial role with regard to customer content, thus became publishers and legally responsible for libel and other torts committed by customers. This act was passed to specifically enhance service providers' ability to delete or otherwise monitor content without themselves becoming publishers.

In Zeran vs. America Online, Inc., the Court notes that "Congress enacted § 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.

In Carafano vs. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003), the court upheld immunity for an Internet dating service provider from liability stemming from third party's submission of false profile. The plaintiff, Carafano, claimed the false profile defamed her, but because the content was created by a third party, the website was immune, even though it had provided multiple choice selections to aid profile creation.

In Batzel vs. Smith, 333 F.3d 1018 (9th Cir. 2003), Immunity was upheld for a website operator for distributing an e-mail to a listserv where the plaintiff claimed the e-mail was defamatory. Though there was a question as to whether the information provider intended to send the e-mail to the listserv, the Court decided that for determining the liability of the service provider, "the focus should be not on the information provider's intentions or knowledge when transmitting content but, instead, on the service provider's or user's reasonable perception of those intentions or knowledge." The Court found immunity proper "under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other 'interactive computer service'."

In Goddard vs. Google, Inc., C 08-2738 JF (PVT), 2008 WL 5245490, 2008 U.S. Dist. LEXIS 101890 (N.D. Cal. Dec. 17, 2008), Immunity upheld against claims of fraud and money laundering. Google was not responsible for misleading advertising created by third parties who bought space on Google's pages. The court found the creative pleading of money laundering did not cause the case to fall into the crime exception to Section 230 immunity.

In Doe vs. MySpace, 528 F.3d 413 (5th Cir. 2008), The court upheld immunity for a social networking site from negligence and gross negligence liability for

[23] http://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act

failing to institute safety measures to protect minors and failure to institute policies relating to age verification. The Does' daughter had lied about her age and communicated over MySpace with a man who later sexually assaulted her. In the court's view, the Does' allegations were "merely another way of claiming that MySpace was liable for publishing the communications."

In Fair Housing Council of San Fernando Valley vs. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc), the Ninth Circuit Court of Appeals rejected immunity for the Roommates.com roommate matching service for claims brought under the federal Fair Housing Act and California housing discrimination laws. The court concluded that the manner in which the service elicited information from users concerning their roommate preferences (by having dropdowns specifying gender, presence of children and sexual orientation) and the manner in which it utilized that information in generating roommate matches (by eliminating profiles that did not match user specifications), the matching service created or developed the information claimed to violate the FHA and thus was responsible for it as an "information content provider." The court upheld immunity for the descriptions posted by users in the "Additional Comments" section because these were entirely created by users.

[24]This legal regime institutes ISP liability rules not only for torts but also for all types of illegitimate activities in cyberspace that are "initiated by third parties on-line (e.g. copyright piracy, unfair competition, misleading advertising)." The European Union's Electronic Commerce Directive's "notice, take-down and put-back" regime would compel an ISP to remove tortious or other objectionable material. The Directive supplements national takedown policies already in force in some European countries. Tennis star Steffi Graf, for example, prevailed in a lawsuit against Microsoft after the Internet Service Provider refused to remove doctored digital images of her in pornographic poses on its "Celebrities" chat room.

The Graf court found Microsoft to be "responsible for the content posted to its server because it provided the infrastructure, established the topic, permitted the posting over its own Web pages and established the basic rules." In the United States, Section 230 of the Communications Decency Act (CDA) would have immunized Microsoft for merely permitting a posting on its services.

Similarly, in Godfrey vs. Demon Internet, a service provider claimed it was entitled to an innocent disseminator defense under the United Kingdom's 1996 Defamation Act. The court stripped the ISP of its immunity since it did not take down defamatory material even after being notified three times. In the United States, no court has held a service provider liable for failing to expeditiously remove defamatory material. In this British case, the ISP settled the defamation claim for approximately "$25,000 in damages plus plaintiff's costs and fees (likely to be several hundred thousand dollars)."

3.10 CYBER TORT IN FRANCE

In **LICRA vs. Yahoo!**, the High Court ordered Yahoo! to take affirmative steps to filter out Nazi memorabilia from its auction site. Yahoo!, Inc. and its then president Timothy Koogle were also criminally charged, but acquitted.

Upon noticing the continued presence of revisionist and anti-semitic material on sale or otherwise observable on the yahoo.com site, French associations dedicated to combatting anti-semitism and racism brought fresh actions against Yahoo Inc. and its then President, Timothy Koogle, for a range of infractions under French

[24] http://www.law.suffolk.edu/faculty/add/infor/ustad04_JHTL_Lambert_RustadKoenig.pdf

criminal laws such as apology of war crimes. The defendants unsuccessfully challenged the jurisdiction of the French court but were acquitted of the criminal charges because the conduct reproached of them did not correspond to the elements required to prove guilt of the crimes for which they were charged. On appeal, the judgment was confirmed in that the defendants were judged to be subject to the court's jurisdiction and French law was applied to them, but they were found not guilty of the charges[25].

3.11 CYBER TORT IN USA[26]

The extent to which tort law has evolved to continue its traditional redress for individuals injured by the wrongful acts of others has been severely restricted in the case of some torts, particularly when the act is one involving third party content and service providers. As Rustad and Koenig (2005) noted, despite "rosy prediction that new torts were on the horizon to protect consumers in cyberspace. We were mistaken. Tort law has yet to expand to defend the consuming public against a wide variety of wrongdoing on the World Wide Web because of the overly broad immunity conferred on ISPs."

In the United States, federal restrictions provide immunity for many activities in the context of cyberspace. Many of these activities have been traditionally governed and adjudicated according to common law tort principles. When the cases relate to property interests, the common law is adapted. When the torts alleged relate to individual interests, federal laws and the expansive interpretation of their application have limited the evolutionary path of the common law.

3.11.1 The Communications Decency Act and Tort Claims for Injury to Person

In Doe vs. AOL, Inc. (2001), the State Supreme Court of Florida was called upon to provide answers to a "question of great public importance." The issue was whether or not the Communications Decency Act (CDA) had preempted certain state common law tort actions. The questions were based on a case filed by the mother of a minor child, who alleged that AOL was negligent in its oversight of its service when it failed to recognize or take action against a subscriber who was using the service to market and distribute child pornography. Emotional injuries were suffered by the plaintiff's son when the offender used the service to lure him to participate in his activities. The trial court and intermediate court of appeals dismissed the plaintiff's action, citing prevailing federal case law under the CDA. Section 230 of that act provides:

"(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of--

(A) any action voluntarily taken in good faith to restrict access to or availability

[25] http://www.lapres.net/yahweb.html
[26] www.jiclt.com/index.php/jiclt/article

of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) Any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

(d) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18 or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

The court rephrased the certified questions submitted to it and considered them in reverse order. It first answered the question if section 230 preempted state law negligence claims against Internet Service Providers (ISPs) as a distributors of information, that violated state criminal statutes prohibiting the distribution of obscene and pornography material.

3.11.2 Conversion

The New York Supreme Court in Shmueli vs. Corcoran Group (2006) was called to decide whether a computerized list (an electronic document that exists inside a computer as opposed to a tangible document that exists on a piece of paper) can be subject to the tort of conversion. The plaintiff in the case alleged that upon termination of their business relationship, the defendant wrongfully denied plaintiff access and continues to deprive plaintiff access, to various real estate deal and client lists she maintained on the computer furnished to her by defendants. The defendant claimed the common law tort of conversion cannot be applied to intangible property. The decision and rationale in this case exemplify the application and expansion of cornerstone legal principles to new situations found in our highly technical modern world.

The court found that the tort of conversion, that is the wrongful exclusion and retention of a rightful owner's physical property, does apply to an electronic record created by a plaintiff to the same extent it would to a paper record created by a plaintiff. The court explained that a computerized list can "undeniably transform" to a physical document simply by utilizing the printing function of the computer. It reasoned that the common law tort of conversion should not become "extinct" in application to documents maintained on a computer, but should "evolve" in sync with the definitions of documents over time. The recording of data and the creation of documents is not limited to paper. The tort of conversion must respect progress in technology and continue to provide redress when one wrongfully interferes with the ownership of electronic documents.

Although the court in this case admitted that the traditional application of this

common law cause of action has "always centered exclusively on the physical theft of specific, identifiable, corporeal, tangible, personal property", the court went on to explain that when the nature of tangible personal property expanded to include tangible documents that represent intangible rights, such as bank notes, promissory notes, stock certificates and insurance policies, courts began to interpret the tort of conversion to include these paper documents within its scope.

In Hartford Accident & Indem. Co. vs. Walston & Co., Inc. (1967), the court said that the New York Court of Appeals followed the trend when it applied the tort of conversion to the theft of stock. The court in this case found no reason why it should not apply the same logic to the present type of documents. Electronic documents belong to someone and are subject to theft. Therefore, it fell within the scope of the tort of conversion.

The court also referred to two federal decisions and agreed with their reasoning. In Kremen vs. Cohen (2003), the Ninth Circuit permitted the plaintiff's conversion claim regarding its Internet domain name. In Astroworks, Inc. vs. Astroexhibit, Inc. (2003), the District Court for the Southern District of New York allowed the plaintiff to sue the defendant for converting plaintiff's ideas for an Internet, web-based business to defendant's own gain. The intangible nature of the property involved in these cases did not preclude a cause of action for conversion. The court in this case agreed that the historic distinction between tangible and intangible property must be less rigidly applied in order to "keep up with science."

The finding in this case – "that electronically written 'documents' should not be treated with less dignity of ownership for conversion purposes than ink written "documents" was upheld on appeal by the New York Supreme Court Appellate Division.

3.11.3 Misappropriation of Trade Secrets

In Briefing.com vs. Jones, the Supreme Court of Wyoming agreed to answer the following two questions submitted by the United States District Court for the District of Wyoming: "1. Would the Wyoming Supreme Court adopt a common-law cause of action for misappropriation of trade secrets and/or confidential information when the former employees of a company are alleged to have misappropriated their former employer's trade secrets and/or confidential information to start a competing business? 2. If the answer to question number 1 is yes, what are the elements of the cause of action?"The questions resulted from a diversity case filed by a California corporation, an Internet based company that provides stock and fixed income markets analysis for individual and professional investors on its website, against two of its former employees who are Wyoming residents.

The plaintiff alleged that the defendant's utilized trade secrets and/or confidential information gained in their positions with the plaintiff to form and operate a competing business. Specifically the plaintiff claimed that the defendants had access to confidential information and data with respect to the internet based market analysis trade, knowledge of the plaintiff's development and proprietary studies regarding designs and themes and access to market contact information.

The state of Wyoming had not previously considered a case regarding the protection of trade secrets and consequently had not addressed the issue with respect to intangible electronic information and an Internet based company.

The court answered the first question in the affirmative: that common law in the state of Wyoming includes a cause of action for misappropriation of trade secrets and/or confidential information with regard to information gained during employment and used to start a competing Internet business. The court responded

to the second question and ruled that the elements required to support such a cause of action are those found in the restatement (Third) of Unfair Competition. The court reasoned that misuse of trade secrets is a recognized cause of action under common law and that the Wyoming legislature had adopted the common law as applicable in Wyoming more than 100 years ago. In determining the elements of the tort, the court referred to the Restatement (Third) of Unfair Competition and stated that it served to "accommodate the law to developments in the commercial world."

3.11.4 Trespass to Chattels

To establish a common law action for trespass to chattels, a plaintiff must prove that the defendant intentionally and without consent, physically interfered with the use and enjoyment of personal property in the plaintiff's possession and that the plaintiff was thereby harmed. The interference with the chattel must have resulted in harm to the owner's interest in the physical condition, quality or value of the chattel or when the owner is deprived actual use of the chattel for a substantial period of time.

In School of Visual Arts vs. Kuprewicz (2003), the Supreme Court of New York determined whether the common law trespass to chattels applies to a computer system. In CompuServe Inc. vs. Cyber Promotions, Inc. (1997), the sending of unsolicited commercial bulk e-mails supported a claim for trespass to chattels where processing power and disk space were shown to be adversely affected and in Hotmail Corp. vs. Van$ Money Pie Inc. (1998) the plaintiff was determined likely to prevail on a trespass to chattels claim upon having shown that plaintiff's computer storage space was filled up by the defendant's unsolicited e-mails.

In order to prevail with respect to an action for trespass to a computer system, a plaintiff must show that the chattel suffered physical damage. Damage to objects traditionally found in trespass to chattels claims is usually visible and easy to establish. However, the court stated that if physical damage, albeit invisible damage, occurs to the computer system, the plaintiff has a cause of action. Torts that protect property interests, such as conversion, misappropriation of trade secrets and trespass to chattels, can also apply to our highly technical world. Electronic documents, intangible information and invisible systems deserve the same protections as tangible personal property. Courts must modernize their views of the definition of "property" to include these intangible and invisible aspects created by technology.

3.12 CYBER TORT IN AUSTRALIA

The Internet has only been in existence for a few decades, but it has already changed the way people interact. Numerous legal problems have evolved because of acts committed over the Internet. In many areas, the common law has been slow to catch up to the new problems that have arisen with advent of the Internet.

The first case in which the court ruled that a tort was committed using the Internet was in Australia in University of West Australia in Rindos vs. Hardwick[27]. Internet torts are considerably different from the "bricks and mortar world of traditional civil litigation in which family law and personal injury tort cases predominate." A major difference between traditional tort claims and Internet tort claims is the nature of injuries suffered by the plaintiffs. Most cases involving the Internet involve financial loss. Also, ninety-seven percent of Internet torts are intentional torts while traditional torts are predominately negligence.

Scholars have recognized that most torts committed using the Internet are

[27] http://www.ratbags.com/rsoles/onews/rindos.htm

publication or informational torts. This is because a person can use chat rooms, web pages, newsgroups and other technological innovation to make his voice heard. It was recognized, even before SNSs became mainstream, that these technological innovations created the potential for widespread invasions of privacy.

Although the substance of a tort claim is the same for a traditional tort as it is for an Internet tort, there are differences in the two actions. Among the differences are type of remedy sought (predominately money for traditional tort cases but equitable relief in Internet cases) and types of damage (predominately personal injury in traditional cases but economic loss for Internet torts).

3.13 LEGAL ISSUES RELATING TO WIKILEAKS

Wikileaks as a phenomenon has ushered in a new revolution in information disclosure and as time passes by, will be an important element in the further growth of jurisprudence in this regard. Let us now examine legal aspects relating to Wikileaks, which have emerged thanks to the various developments relating to Wikileaks case.

- **Potential Criminal Prosecution**[28]

  The U.S. Justice Department opened a criminal probe of WikiLeaks and founder Julian Assange shortly after the leak of diplomatic cables began. Attorney General Eric Holder affirmed the probe was "not sabre-rattling", but was "an active, ongoing criminal investigation." The Washington Post reported that the department was considering charges under the Espionage Act, a move which former prosecutors characterised as "difficult" because of First Amendment protections for the press. Several Supreme Court cases have previously established that the American constitution protects the re-publication of illegally gained information provided the publishers did not themselves break any laws in acquiring it. Federal prosecutors have also considered prosecuting Assange for trafficking in stolen government property, but since the diplomatic cables are intellectual rather than physical property, that approach also faces hurdles. Any prosecution of Assange would require extraditing him to the United States, a step made more complicated and potentially delayed by any preceding extradition to Sweden. One of Assange's lawyers, however, says they are fighting extradition to Sweden because it might lead to his extradition to the United States. Assange's attorney, Mark Stephens, has "heard from Swedish authorities there has been a secretly empaneled grand jury in Alexandria [Virginia]" meeting to consider criminal charges in the WikiLeaks case.

  In Australia, the government and the Australian Federal Police have not stated what Australian laws may have been broken by WikiLeaks, but Julia Gillard has stated that the foundation of WikiLeaks and the stealing of classified documents from the US administration is illegal in foreign countries. Gillard later clarified her statement as referring to "the original theft of the material by a junior US serviceman rather than any action by Mr Assange." Spencer Zifcak, President of Liberty Victoria, an Australian civil liberties group, notes that with no charge and no trial completed, it is inappropriate to state that WikiLeaks is guilty of illegal activities.

  On threats by various governments toward Assange, legal expert Ben Saul argues that founder Julian Assange is the target of a global smear campaign to demonise him as a criminal or as a terrorist, without any legal basis. The

[28] http://en.wikipedia.org/wiki/WikiLeaks
[29] http://en.wikipedia.org/wiki/WikiLeaks

Center for Constitutional Rights has issued a statement highlighting its alarm at the "multiple examples of legal overreach and irregularities" in his arrest.

- **Insurance file**[29]

On 29 July 2010, WikiLeaks added a 1.4 GB "Insurance File" to the Afghan War Diary page. The file is AES encrypted and has been speculated to serve as insurance in case the WikiLeaks website or its spokesman Julian Assange are incapacitated, upon which the passphrase could be published, similar to the concept of a dead man's switch. Following the first few days' release of the US diplomatic cables starting 28 November 2010, the US television broadcaster CBS predicted that "If anything happens to Assange or the website, a key will go out to unlock the files. There would then be no way to stop the information from spreading like wildfire because so many people already have copies." CBS correspondent Declan McCullagh stated, "What most folks are speculating is that the insurance file contains unreleased information that would be especially embarrassing to the US government if it were released."

In January 2009, WikiLeaks released 86 telephone intercept recordings of Peruvian politicians and businessmen involved in the 2008 Peru oil scandal. In February, WikiLeaks released 6,780 Congressional Research Service reports followed in March, by a list of contributors to the Norm Coleman senatorial campaign and a set of documents belonging to Barclays Bank that had been ordered removed from the website of The Guardian. In July, they released a report relating to a serious nuclear accident that had occurred at the Iranian Natanz nuclear facility in 2009. Later media reports have suggested that the accident was related to the Stuxnet computer worm. In September, internal documents from Kaupthing Bank were leaked, from shortly before the collapse of Iceland's banking sector, which led to the 2008-2010 Icelandic financial crisis. The document shows that suspiciously large sums of money were loaned to various owners of the bank and large debts written off. In October, Joint Services Protocol 440, a British document advising the security services on how to avoid documents being leaked was published by WikiLeaks. Later that month, they announced that a super-injunction was being used by the commodities company, Trafigura to gag The Guardian newspaper from reporting on a leaked internal document regarding a toxic dumping incident in the Ivory Coast. In November, they hosted copies of e-mail correspondence between climate scientists, although they were not originally leaked to WikiLeaks. They also released 570,000 intercepts of pager messages sent on the day of the 11 September attacks. During 2008 and 2009, WikiLeaks published the alleged lists of forbidden or illegal web addresses for Australia, Denmark and Thailand. These were originally created to prevent access to child pornography and terrorism, but the leaks revealed that other sites covering unrelated subjects were also listed.

In March 2010, WikiLeaks released a secret 32-page U.S. Department of Defense Counterintelligence Analysis Report written in March 2008 discussing the leaking of material by WikiLeaks and how it could be deterred. In April, a classified video of the 12 July 2007 Baghdad airstrike was released, showing two Reuters employees being fired at, after the pilots mistakenly thought the men were carrying weapons, which were in fact cameras. In the week following the release, "wikileaks" was the search term with the most significant growth worldwide in the last seven days as measured by Google Insights.[172] In January 2010, WikiLeaks received the first test cable A 22-year-old US Army intelligence analyst, PFC (formerly SPC) Bradley Manning, a US embassy cable relating about IceSave, thereafter referred as "Reykjavik 13"[citation needed]. In June 2010, he was arrested after alleged chat logs were turned in to the authorities by former hacker Adrian Lamo, in whom he had confided. Manning reportedly told Lamo he had leaked the "Collateral Murder" video,

in addition to a video of the Granai airstrike and around 260,000 diplomatic cables, to WikiLeaks. In July, WikiLeaks released 92,000 documents related to the war in Afghanistan between 2004 and the end of 2009 to The Guardian, The New York Times and Der Spiegel. The documents detail individual incidents including friendly fire and civilian casualties. At the end of July, a 1.4 GB "insurance file" was added to the Afghan War Diary page, whose decryption details would be released if WikiLeaks or Assange were harmed. About 15,000 of the 92,000 documents have not yet been released on WikiLeaks, as the group is currently reviewing the documents to remove some of the sources of the information. WikiLeaks asked the Pentagon and human-rights groups to help remove names from the documents to reduce the potential harm caused by their release, but did not receive assistance. Following the Love Parade stampede in Duisburg, Germany on 24 July 2010, a local published internal documents of the city administration regarding the planning of Love Parade. The city government reacted by acquiring a court order on 16 August forcing the removal of the documents from the site on which it was hosted. On 20 August WikiLeaks released a publication titled Loveparade 2010 Duisburg planning documents, 2007-2010, which comprised 43 internal documents regarding the Love Parade 2010. Following on from the leak of information from the Afghan War, in October 2010, around 400,000 documents relating to the Iraq War were released in October. The BBC quoted The Pentagon referring to the Iraq War Logs as "the largest leak of classified documents in its history." Media coverage of the leaked documents focused on claims that the U.S. government had ignored reports of torture by the Iraqi authorities during the period after the 2003 war.

- **Diplomatic cables release**[30]

On 28 November 2010, WikiLeaks and five major newspapers from Spain (El País), France (Le Monde), Germany (Der Spiegel), the United Kingdom (The Guardian) and the United States (The New York Times) started to simultaneously publish the first 220 of 251,287 leaked confidential-but not top secret-diplomatic cables from 274 US embassies around the world, dated from 28 December 1966 to 28 February 2010. WikiLeaks plans to release the entirety of the cables in phases over several months.

The contents of the diplomatic cables include numerous unguarded comments and revelations regarding: critiques and praises about the host countries of various US embassies; political manoeuvring regarding climate change; discussion and resolutions towards ending ongoing tension in the Middle East; efforts and resistance towards nuclear disarmament; actions in the War on Terror; assessments of other threats around the world; dealings between various countries; US intelligence and counterintelligence efforts; and other diplomatic actions. Reactions to the United States diplomatic cables leak include stark criticism, anticipation, commendation and quiescence. Consequent reactions to the US government include sympathy, bewilderment and dismay. On 14 December 2010 the United States Department of Justice issued a subpoena directing Twitter to provide information for accounts registered to or associated with WikiLeaks. Twitter decided to notify its users.The overthrow of the presidency in Tunisia has been attributed in part to reaction against the corruption revealed by leaked cables.

In May 2010, WikiLeaks said they had video footage of a massacre of civilians in Afghanistan by the US military which they were preparing to release.

In an interview with Chris Anderson on 19 July 2010, Assange showed a document WikiLeaks had on an Albanian oil well blowout and said they also

[30] http://en.wikipedia.org/wiki/WikiLeaks

had material from inside BP and that they were "getting enormous quantity of whistle-blower disclosures of a very high calibre" but added that they have not been able to verify and release the material because they do not have enough volunteer journalists.

In October 2010, Assange told a leading Moscow newspaper that "The Kremlin had better brace itself for a coming wave of WikiLeaks disclosures about Russia." Assange later clarified: "we have material on many businesses and governments, including in Russia. It's not right to say there's going to be a particular focus on Russia".

In a 2009 Computer World interview, Assange claimed to be in possession of "5GB from Bank of America". In 2010 he told Forbes magazine that WikiLeaks was planning another "megaleak" early in 2011, from inside the private sector, involving "a big U.S. bank" and revealing an "ecosystem of corruption". Bank of America's stock price fell by 3% as a result of this announcement. Assange commented on the possible impact of the release that "it could take down a bank or two."

In December 2010, Assange's lawyer, Mark Stephens, told The Andrew Marr Show on the BBC, that WikiLeaks had information it considers to be a "thermo-nuclear device" which it would release if the organisation needs to defend itself.

In January 2011, Rudolf Elmer, a former Swiss banker, passed on data containing account details of 2,000 prominent people to Assange, who stated that the information will be vetted before being made publicly available at a later date.

On 3 December, 2010, PayPal, the payment processor owned by eBay, permanently cut off the account of the Wau Holland Foundation that had been redirecting donations to WikiLeaks. PayPal alleged that the account violated its "Acceptable Use Policy", specifically that it was used for "activities that encourage, promote, facilitate or instruct others to engage in illegal activity." The Vice President of PayPal later stated that they stopped accepting payments after the "State Department told us these were illegal activities. It was straightforward." Later the same day, he said that his previous statement was incorrect and that it was in fact based on a letter from the State Department to WikiLeaks. On 8 December 2010, the Wau Holland Foundation released a press statement, saying it has filed a legal action against PayPal for blocking its account used for WikiLeaks payments and for libel due to PayPal's allegations of "illegal activity"..

On 6 December 2010, the Swiss bank, PostFinance, announced that it had frozen the assets of Assange that it holds, totalling 31,000. In a statement on their website, they stated that this was because Assange "provided false information regarding his place of residence" when opening the account. WikiLeaks released a statement saying this was due to that Assange, "as a homeless refugee attempting to gain residency in Switzerland, had used his lawyer's address in Geneva for the bank's correspondence".

On the same day, MasterCard announced that it was "taking action to ensure that WikiLeaks can no longer accept MasterCard-branded products", adding "MasterCard rules prohibit customers from directly or indirectly engaging in or facilitating any action that is illegal." The next day, Visa Inc. announced it was suspending payments to WikiLeaks, pending "further investigations". In a move of support for WikiLeaks, XIPWIRE established a way to donate to WikiLeaks and waived their fees. Datacell, the Swiss-based IT company that enabled WikiLeaks to accept credit card donations, announced that it will

take legal action against Visa Europe and Mastercard, in order to resume allowing payments to the website.

On 18 December, Bank of America announced it would "not process transactions of any type that we have reason to believe are intended for Wikileaks," citing "Wikileaks might be engaged in activities inconsistent with our internal policies for processing payments". WikiLeaks responded in a tweet by encouraging their supporters who were BoA customer to close their accounts. Bank of America has long been believed to be the target of WikiLeaks' next major release. Late in 2010, Bank of America approached the law firm of Hunton & Williams to put a stop to WikiLeaks. Hunton & Williams assembled a group of security specialists, HBGary Federal, Palantir Technologies and Berico Technologies. They decided upon a campaign of dirty tricks, which included "false documents, disinformation and sabotage." HBGary Federal's CEO Aaron Barr wrote Palintir that security companies should track and intimidate people who donate to WikiLeaks."Security firms need to get people to understand that if they support the organisation we will come after them."

During the 5th and 6th of February 2011, Anonymous hacked HBGary's web site, copied tens of thousands of documents from HBGary, posted tens of thousands of company e-mails online and usurped Barr's Twitter account in revenge. Some of the documents taken by Anonymous show HBGary Federal was working on behalf of Bank of America to respond to Wikileaks' planned release of the bank's internal documents. E-mails detailed a supposed business proposal by HBGary to assist Bank of America's law firm, Hunton & Williams, revealed the companies were willing to break the law to bring down WikiLeaks and Anonymous.

- **People's Republic of China**[31]

  The WikiLeaks website claims that the government of the People's Republic of China has attempted to block all traffic to web sites with "wikileaks" in the URL since 2007, but that this can be bypassed through encrypted connections or by using one of WikiLeaks' many covert URLs.

- **Australia**[32]

  On 16 March 2009, the Australian Communications and Media Authority added WikiLeaks to their proposed blacklist of sites that will be blocked for all Australians if the mandatory internet filtering censorship scheme is implemented as planned. The blacklisting was removed 30 November 2010.

- **Thailand**[33]

  The Centre for the Resolution of the Emergency Situation (CRES) is currently censoring the website WikiLeaks in Thailand and more than 40,000 other webpages because of the emergency decree in Thailand imposed as a result of political instabilities (Emergency decree declared beginning of April 2010.

- **Iceland**[34]

  After the release of the 2007 airstrikes video and as they prepared to release film of the Granai airstrike, Julián Assange has said that his group of volunteers came under intense surveillance. In an interview and Twitter posts he said

[31] http://en.wikipedia.org/wiki/WikiLeaks
[32] http://en.wikipedia.org/wiki/WikiLeaks
[33] http://en.wikipedia.org/wiki/WikiLeaks
[34] http://en.wikipedia.org/wiki/WikiLeaks

that a restaurant in Reykjavík where his group of volunteers met came under surveillance in March; there was "covert following and hidden photography" by police and foreign intelligence services; that an apparent British intelligence agent made thinly veiled threats in a Luxembourg car park; and that one of the volunteers was detained by police for 21 hours. Another volunteer posted that computers were seized, saying "If anything happens to us, you know why and you know who is responsible." According to the Columbia Journalism Review, "the Icelandic press took a look at Assange's charges of being surveilled in Iceland [...] and, at best, have found nothing to substantiate them."

In August 2009, Kaupthing Bank succeeded in obtaining a court order gagging Iceland's national broadcaster, RÚV, from broadcasting a risk analysis report showing the bank's substantial exposure to debt default risk. This information had been leaked by a whistleblower to WikiLeaks and remained available on the WikiLeaks site; faced with an injunction minutes before broadcast the channel ran with a screen grab of the WikiLeaks site instead of the scheduled piece on the bank. Citizens of Iceland felt outraged that RÚV was prevented from broadcasting news of relevance.Therefore, WikiLeaks has been credited with inspiring the Icelandic Modern Media Initiative, a bill meant to reclaim Iceland's 2007 Reporters Without Borders (Reporters sans frontières) ranking as first in the world for free speech. It aims to enact a range of protections for sources, journalists and publishers. Birgitta Jónsdóttir, a former volunteer for WikiLeaks and member of the Icelandic parliament, is the chief sponsor of the proposal.

- **United States**[35]

Access to WikiLeaks is currently blocked in the United States Library of Congress. On 3 December 2010 the White House Office of Management and Budget sent a memo forbidding all unauthorised federal government employees and contractors from accessing classified documents publicly available on WikiLeaks and other websites. The U.S. Army, the Federal Bureau of Investigation and the Justice Department are considering criminally prosecuting WikiLeaks and Assange "on grounds they encouraged the theft of government property", although former prosecutors say doing so would be difficult. According to a report on the Daily Beast website, the Obama administration asked Britain, Germany and Australia among others to also consider bringing criminal charges against Assange for the Afghan war leaks and to help limit Assange's travels across international borders. Columbia University students have been warned by their Office of Career Services that the U.S. State Department had contacted the office in an e-mail saying that the diplomatic cables which were released by WikiLeaks were "still considered classified." and that "online discourse about the documents would call into question your ability to deal with confidential information." All U.S. federal government staff has been blocked from viewing WikiLeaks. Some Department of Homeland Security staff say the ban on accessing WikiLeaks on government computers and other government devices is hampering their work; "More damage will be done by keeping the federal workforce largely in the dark about what other interested parties worldwide are going to be reading and analyzing." One official says that the ban apparently covers personal computers also.

There are a lot of complicated legal issues that impact the activities of Wikileaks. These issues are in a state of development at the time of writing. However, Wikileaks legal issues promise to have a profound impact upon the growth of relevant legal jurisprudence.

[35] http://en.wikipedia.org/wiki/WikiLeaks

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain Different Types of Cyber Tort.

.....

.....

.....

.....

2) Explain Tortious liability in Cyber Crimes.

.....

.....

.....

.....

3) Write short note on "Right of Publicity".

.....

.....

.....

.....

3.14 LET US SUM UP

This unit deals with the tort involved in the cyberspace or committed on a computer network. Torts or Civil wrongs are wrongs committed against private entities such as companies or private citizens, but are not necessarily offences against the state. Cyber Tort is a tort committed in cyberspace. Cyber crimes are the crimes which targets the computer database and systems. They usually 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.

3.15 CHECK YOUR PROGRESS: THE KEY

1) **Cyber Stalking** – Cyber stalking occurs when a person is followed and persuaded online. In other words, their privacy is invaded. It is a form of harassment and can disrupt the life of the victim leaving them feeling afraid and threatened.

In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications. Harassment can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender. Harassment may also include threats, sexual remarks, pejorative labels (i.e. hate speech).

A particularly disturbing form of harassment is sending a forged e-mail that appears to be from the victim and contains racist remarks or other embarrassing text, that will tarnish the reputation of the victim.

2) Cyber crime is a kind of crime in which generally offenders of crimes are generally hidden. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of other countries. Basic liability in cyber crime is established through the principle of neighbourhood established from the case of donoghue vs. stevenson. The major liability in cyber tort in India is through Information Technology Act, 2000 (as amended).

   Victim(s) of computer crimes can sue the perpetrator in tort. For example, unauthorized use of a computer system could be "trespass on chattels". A computer voyeur might also be sued in tort for invasion of privacy or disclosure of a trade secret. A harasser might be sued in tort for intentional infliction of emotional distress. There is also the possibility of a class action by corporate and personal victims against a person who wrote and initially released a computer virus.

   There is another remedy in civil law, besides damages awarded in tort litigation: a victim can get a temporary restraining order (TRO), then an injunction, that enjoins continuance of wrongs (e.g. disclosure of proprietary or private data) that will cause irreparable harm or for which there is no adequate remedy at law.

3) Refer to Section 3.8

UNIT 4 CRIMES RELATING TO DATA ALTERATION/ DESTRUCTION/THEFT OF SOURCE CODE AND DATABASE

Structure

4.0 INTRODUCTION

Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Additionally, although the terms computer crime and cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important[1].

4.1 OBJECTIVES

After going through this Unit, you should be able to:

- explain data destruction and its methods;
- explain ODR and its methods;

[1] http://sawaal.ibibo.com/computers-and-technology/illegal-way-damage-computer-system-781097.html

- understand European Union Convention on cybercrime; and
- explain offences against the confidentiality, integrity and availability of computer data and systems.

4.2 COMPUTER CRIME

The world of Internet today has become a parallel form of life and living because with the availability of artificial intelligence and new technologies, we are now capable of doing things which were not even imaginable few years ago[2]. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. The advent of the computer has been a boon to students, lawyers, businessmen, teachers, doctors, researchers and also, of course, to the criminals.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft) and electronic fraud[3].

Computer crime issues have become high-profile, particularly those surrounding hacking, copyright infringement through warez, child pornography and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Unauthorized access, damage to property, theft, fraud, mischief and the publication of obscene and indecent material are all familiar crimes. The expression "crime" is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. With the emergence of Internet, the traditional crimes have assumed new dimensions[4].

A common example is when a person starts to steal information from sites or cause damage to, a computer or computer network. This can be entirely virtual in that the information only exists in digital form and the damage, while real, has no physical consequence other than the machine ceases to function.

Computer crime encompasses a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories[5]:

(1) Crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Examples of crimes that primarily target computer networks or devices would include,

[2] http://www.amarjitassociates.com/articles/cybercrimes-1.htm

[3] http://sawaal.ibibo.com/computers-and-technology/illegal-way-damage-computer-system-781097.html

[4] http://www.amarjitassociates.com/articles/cybercrimes-1.htm

[5] http://sawaal.ibibo.com/computers-and-technology/illegal-way-damage-computer-system-781097.html

* Malware and malicious code

* Denial-of-service attacks

* Computing viruses

Examples of crimes that merely use computer networks or devices would include,

* Cyber stalking

* Fraud and identity theft

* Phishing scams

* Information warfare

Clearing: Clearing is the removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities.

Purging: Purging or sanitising is the removal of sensitive data from a system or storage device with the intent that the data can not be reconstructed by any known technique.

Destruction: The storage medium is physically destroyed. Effectiveness of physical destruction varies. Depending on recording density of the medium and/or the destruction technique, this may leave data recoverable by laboratory methods[6].

4.3 DATA ALTERATION[7]

It is the intentional use of illegal and destructive programs to alter or destroy data.

Virus: A program that attaches itself to other programs. A virus cannot run by itself, but infects other programs. The simplest virus only reproduces itself. Anything more is called payload which can be anything from a cute message ("Hi, you're infected (:-o)) to erasing your hard drive. Really nasty payloads are rare: the viruses kill themselves before they spread all over the world.

Worm: An independent program that replicates its own program files until it destroys other systems and programs or interrupts the operation of networks and computer systems.

Trojan: A program which appears to do one thing but has a destructive payload hidden inside

Example: an old Trojan started to draw a photo of a woman, head and legs first; before it reached the middle, it had erased the hard drive

Example: a program that appears to be the usual network logon, but is actually e-mailing usernames and passwords to a cracker.

Data-stealing malware[8]

Data-stealing malware is a web threat that divests victims of personal and proprietary information with the intent of monetizing stolen data through direct use or underground distribution. Content security threats that fall under this umbrella include keyloggers, screen scrapers, spyware, adware, backdoors and bots. The term does not refer to activities such as spam, phishing, DNS poisoning, SEO

[6] http://en.wikipedia.org/wiki/Data_remanence

[7] http://facpub.stjohns.edu~wolfem/4322Chapter14.htm

[8] http://en.wikipedia.org/wiki/Malware

abuse etc. However, when these threats result in file download or direct installation, as most hybrid attacks do, files that act as agents to proxy information will fall into the data-stealing malware category.

Data-stealing malware incidents

A Trojan horse program stole more than 1.6 million records belonging to several hundred thousand people from Monster Worldwide Inc's job search service. The data was used by cybercriminals to craft phishing e-mails targeted at Monster.com users to plant additional malware on users' PCs.

Customers of Hannaford Bros. Co, a supermarket chain based in Maine, were victims of a data security breach involving the potential compromise of 4.2 million debit and credit cards. The company was hit by several class-action law suits.

The Torpig Trojan has compromised and stolen login credentials from approximately 250,000 online bank accounts as well as a similar number of credit and debit cards. Other information such as e-mail and FTP accounts from numerous websites, have also been compromised and stolen.

4.4 SOURCE CODE THEFT[9]

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies. As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations that get original software developed for their use.

In first case, the source code theft the suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

The suspect is an employee of the victim; he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then contact potential buyers to make the sale.

In the second case, the suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software. If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device then modify the source code (either himself or in association with other programmers) and launch his own software.

If the person committed the offence of source code theft he shall be punished under Sections 43, 65 & 66 of the Indian Information Technology Act, 2000 and section 63 of Copyright Act. But after the amendment of the IT Act he shall be punished under Sections 43, 65, 66 & 66B of the Information Technology Act and section 63 of Copyright Act as also punishable under the Indian Penal Code.

Tampering with Computer Source Code[10]

According to section 65 of the IT Act, "Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal,

[9] http://www.cyberlawdb.com/main/india/cyber-crime-law64-source-code-theft.htm

[10] http://www.asianlaws.org/library/cyber-laws/tampering-with-computer-source-code.pdf

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. Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."

Computer source code need not only be in the electronic form. It can be printed on paper e.g. printouts of flowcharts for designing a software application.

The following acts are prohibited in respect of the source code:

1) knowingly concealing or destroying or altering

2) intentionally concealing or destroying or altering

3) knowingly causing another to conceal or destroy or alter

4) intentionally causing another to conceal or destroy or alter

5) Conceal simply means "to hide".

A has created a software program. The source code files of the program are contained in a folder on A's laptop. B changes the properties of the folder and makes it a "hidden" folder. Although the source code folder still exists on A's computer, she can no longer see it. B has concealed the source code.

Destroys means "to make useless", "cause to cease to exist", "nullify", "to demolish" or "reduce to nothing". Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Alters, in relation to source code, means "modifies", "changes","makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc.

The case of **"Syed Asifuddin and Ors. vs. The State of Andhra Pradesh and Anr"** is an important case to examine in this regard.

Facts of the case

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically "unlocked" so that the exclusive Reliance handsets could be used for the Tata Indicom service. Reliance officials came to know about this "unlocking" by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for reprogramming the Reliance handsets. These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defence

1) Subscribers always had an option to change from one service provider to another.

2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4) A telephone handset is neither a computer nor a computer system containing a computer programme.

5) There is no law in force which requires the maintenance of "computer source code". Hence, Section 65 of the Information Technology Act does not apply.

Findings of the court

1) As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2) The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4) When the person moves from one cell to another cell in the same city, the system i.e. Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Conclusions of the court

1) A cell phone is a computer as envisaged under the Information Technology Act.

2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –

   a) "when the computer source code is required to be kept"

   b) "maintained by law for the time being in force"

At the international level, the Convention on Cybercrime of the Council of Europe is the living example of a single international treaty on the subject of cybercrimes.

4.5 EUROPEAN UNION CONVENTION ON CYBERCRIME[11]

The criminal offences defined under (Articles 2-6) of the Convention on Cybercrime of the Council of Europe are intended to protect the confidentiality, integrity and

[11] http://conventions.coe.int/treaty/en/reports/html/185.htm

availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks or legitimate and common operating or commercial practices.

Illegal access (Article 2)

"Illegal access" covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.

"Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right".

The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots' to locate and retrieve information on behalf of communication. The application of such tools per se is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it.

Many national legislations already contain provisions on "hacking" offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach

requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

Let us now look at various examples of national legislations impacting or touching upon the subject under discussion.

Georgia Computer Systems Protection Act, 1991

This act establishes certain acts involving computer fraud or abuse as crimes punishable by defined fines or imprisonment or both. This Act provides as follows:

11) 'Without authority' includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network.

a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

   1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

   2) Obtaining property by any deceitful means or artful practice; or

   3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

b) Computer Trespass. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

   1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

   2) Obstructing, interrupting or in any way interfering with the use of a computer program or data; or

   3) Altering, damaging or in any way causing the malfunction of a computer, computer network or computer program, regardless of how long the alteration, damage or malfunction persists shall be guilty of the crime of computer trespass.

North Carolina

N.C.G.S. §14-455. Damaging computers, computer programs, computer systems, computer networks and resources:

a) It is unlawful to willfully and without authorization alter, damage or destroy a computer, computer program, computer system, computer network or any part thereof. A violation of this subsection is a Class G felony if the damage caused

by the alteration, damage or destruction is more than one thousand dollars ($ 1,000). Any other violation of this subsection is a Class 1 misdemeanor.

a) It is unlawful to willfully and without authorization alter, damage or destroy a government computer. A violation of this subsection is a Class F felony.

b) This section applies to alteration, damage or destruction effectuated by introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system or computer network.

CANADA[12]

From a Canadian perspective, the most appropriate definitions may be those contained in the Council of Europe – Convention on Cybercrime. Canada contributed and is a signatory, to this international of criminal offences involving the use of computers:

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences;
- Offences related to infringements of copyright and related rights; and
- Ancillary liability.

Canada is also a signatory to the Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.

The Criminal Code of Canada contains a set of laws dealing with computer crime issues.

As Canada has not yet ratified the Convention on Cybercrime its Criminal Code may not fully address the areas of criminal law set out in the Convention on Cybercrime.

4.6 OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND SYSTEMS

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices

Computer-related offences

- Computer-related forgery
- Computer-related fraud

[12] http://en.wikipedia.org/wiki/Computer_crime_in_Canada

Content-related offences

- Offences related to child pornography

Offences related to infringements of copyright and related rights

Ancillary liability

- Attempt and aiding or abetting
- Corporate liability

[13]Criminal Code of Canada Section 342 is stated in part IX which is called 'Offences against Rights of Property'. It deals specifically with 'Offences Resembling Theft'. This criminal code is closely related with how computer crime is defined and handled in Canada.

There are currently four parts of Section 342 of the Criminal Code of Canada:

Section 342 deals with theft, forgery of credit cards.

Section 342.01 deals with Making, having or dealing in instruments for forging or falsifying credit cards.

Section 342.1 deals with unauthorized use of computer

Section 342.2 deals with Possession of device to obtain computer service

Section 342: Section 342 makes possessing unauthorized credit data and trafficking in credit card passwords an offence. The criminal code states:

Every person who:

a) steals a credit card,

b) forges or falsities a credit card,

c) possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered

   i) by the commission in Canada of an offence or

   ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence or

d) uses a credit card knowing that it has been revoked or canceled.
is guilty of:

   i) an indictable offence and is liable to imprisonment for a term not exceeding ten years or

   ii) an offence punishable on summary conviction.

In this section "traffic" means, in relation to a credit card or credit data, to sell, export from or import into Canada, distribute or deal in any other way.

Section 342.01: This section says that any transaction and possession of any instruments that is intended for use in forging or falsifying credit card is illegal. The full definition of this criminal code states:

Every person who, without lawful justification or excuse,

a) makes or repairs,

---

[13] http://en.wikipedia.org/wiki/Criminal_code_section_342

b) buys or sells,

c) exports from or imports into Canada or

d) possesses any instrument, device, apparatus, material or thing that the person knows has been used or knows is adapted or intended for use in forging or falsifying credit cards

is guilty of:

i) an indictable offence and liable to imprisonment for a term not exceeding ten years or

ii) an offence punishable on summary conviction.

Section 342.1: Unauthorized use of computer is often used to laid charges for hacker or someone who is involved in computer related offences. This section states:

Every one who, fraudulently and without colour of right,

a) obtains, directly or indirectly, any computer service,

b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system or

d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)

is guilty of:

i) an indictable offence and liable to imprisonment for a term not exceeding ten years or

ii) an offence punishable on summary conviction.

Additional Information

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that or a group of interconnected or related devices one or more of which,

a) contains computer programs or other data and

b) pursuant to computer programs,

i) performs logic and control and

ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system or acquire the substance, meaning or purport thereof;

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

Section 342.2: This section says that any transaction and possession of any instruments that is intended for committing offence under section 342.1 is illegal. The full definition of this criminal code states:

Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

is guilty of:

a) an indictable offence and liable to imprisonment for a term not exceeding two years or

b) an offence punishable on summary conviction.

United Kingdom[14]

The first piece of UK legislation designed to specifically address computer misuse was the Computer Misuse Act 1990. The act was a response to growing concern that existing legislation was inadequate for dealing with hackers. The issue was thrown into sharp relief by the failure to convict Stephen Gold and Robert Schifreen who gained unauthorized access to BT's Prestel service in 1984 and were charged under the Forgery and Counterfeiting Act 1981. However, they were acquitted by the Court of Appeal and the acquittal decision was later upheld by the House of Lords.

The Computer Misuse Act 1990, 'an Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes', set out three computer misuse offences.

Unauthorised access to computer material

Unauthorised access with intent to commit or facilitate commission of further offences

Unauthorised modification of computer material

The maximum prison sentences specified by the act for each offence were six months, five years and five years respectively (Amendments to the Computer Misuse Act, introduced in the Police and Justice Act 2006. The first prosecution of an individual for distributing a computer virus came in 1995.

[14] http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_ review_of _UK_computer_crime_legislation

Christopher Pile, aka 'the Black Baron' pleaded guilty to eleven charges under sections 2 and 3 of the Computer Misuse Act and received an 18 month prison sentence. Pile created the viruses Pathogen and Queeg. Both pieces of malware implemented his SMEG (Simulated Metamorphic Encryption Generator) polymorphic engine, making them hard to detect and both were designed to trash substantial portions of a victim's hard drive. He planted the viruses on bulletin boards disguised as games and, in one case, as an anti-virus program. It was estimated that the viruses caused damage amounting to £1 million (The Independent, 16 November 1995).

Spam, Malware and the Law

Practically everyone with an e-mail account is forced to deal with spam. However, the problem of spam isn't limited to nuisance value, wasted bandwidth or inappropriate content. Spam is also used to deliver malicious code; spam messages are often a springboard for 'drive-by downloads' as they can contain links to web sites which cybercriminals have infected with malicious code. Spam is also the primary mechanism used by phishers to direct their victims to fake web sites from which confidential data is then harvested.

To try and address the problem of spam, the Department for Trade and Industry introduced the (Privacy and Electronic Regulations (EC Directive) 2003). These regulations, the UK implementation of EU directive 2002/58/EC are enforced by the Information Commissioner's Office, the UK's independent authority set up to promote access to official information and to protect personal information.

According to the regulations, companies must get an individual's permission before sending e-mail or SMS messages. On the subject of e-mail, the law states that 'a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by or at the instigation of, the sender.'

However, there are significant limitations. In the first place, the regulations only apply to messages sent to individuals' e-mail addresses, not business addresses. The penalties are also limited, when compared to penalties for offences covered by the Computer Misuse Act. Breaches of the regulations must be reported to the Information Commissioner's Office, which is responsible for deciding whether or not to take the offending organization to court. The offending organization may be fined up to £5,000 in a magistrates' court or up to an unlimited amount if the case is referred to trial by jury.

There is also a more serious limitation. The legislation only applies to senders within the UK. This highlights a key problem with all measures designed to deal with cybercriminals: geo-political restrictions on legislation and law enforcement bodies mean they are unable to operate across boundaries and legal jurisdictions, in contrast to cybercriminals.

The Police and Justice Act 2006 (which covers broader issues than computer crime alone) included amendments to the Computer Misuse Act. The maximum prison sentence under section 1 of the original Act was increased from six months to two years. Section 3 of the Act ('unauthorised modification of computer material') was amended to read 'unauthorised acts with intent to impair or with recklessness as to impairing, operation of computer etc.' and carries a maximum sentence of ten years.

The Act also added another section, 'Making, supplying or obtaining articles for use in computer misuse offences', carrying a maximum sentence of two years. This section states:

A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit or to assist in the commission of, an offence under section 1 or 3.

A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit or to assist in the commission of, an offence under section 1 or 3.

A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit or to assist in the commission of, an offence under section 1 or 3.

In this section "article" includes any program or data held in electronic form.

4.7 CRIME AND PUNISHMENT

It's clear that the existence of legislation which addresses specific types of criminal activity is not, in itself, sufficient to tackle the problem of cybercrime. It's also essential to ensure that the police understand the problem and have the resources to deal with it. Unfortunately, in the years following the introduction of the Computer Misuse Act, few UK police authorities outside the Metropolitan Police area had the knowledge and expertise to deal with computer crime; and it was only when it became clear that cybercrime was an issue that wasn't going to go away that resources were put into creating a dedicated agency to address the problem

In April 2001, the government established the National Hi-Tech Crime Unit. Designed to provide a co-ordinated response to cybercrime, it worked closely with specialists from a range of agencies, including the National Crime Squad, HM Revenue and Customs and the National Criminal Intelligence Service.

In April 2006 the NHTCU's responsibilities were taken over by the Serious Organised Crime Agency (SOCA). This resulted in growing concern that there would be fewer resources dedicated to tackling cybercrime as this would only be a small part of SOCA's remit (SOCA aims).

The first is the creation in 2009 of the Police Central ecrime Unit (PCeU). This body is not designed to replace SOCA or other police agencies, but to co-ordinate the response to cybercrime and to provide 'a national investigative capability for the most serious e-crime incidents' (PCeU mission statement). Second is the introduction, also planned for late in 2009 (Hansard [House of Commons debates], 26 February 2009), of the National Fraud Reporting Centre, to provide the public and small businesses with a way to report non-urgent fraud, online or by telephone.

Of course, even where there's a well-developed legal framework and dedicated law enforcement agencies designed to tackle cybercrime, criminals can only be arrested and prosecuted if there is sufficient evidence to bring a case. This is not always straightforward. Unfortunately, not everyone wants to admit they have fallen victim to cybercriminal activity. This is especially true of businesses as such an admission could damage the company's reputation.

USA[15]

The first truly comprehensive federal computer crime statute was the Computer Fraud and Abuse Act of 1986 (CFAA). The statute was the rewritten version of a 1984 statute that proved inadequate in dealing with the problem of computer crime.

[15] http://groups.csail.mit.edu/mac/classes/6.805/articles/rasch-comp-law.html

The act amended Title 18 United States Code Section 1030 to enhance penalties for six types of computer activities: the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or give advantage to a foreign nation; the unauthorized access of a computer to obtain protected financial or credit information; the unauthorized access into a computer used by the federal government; the unauthorized interstate or foreign access of a computer system with an intent to defraud; the unauthorized interstate or foreign access of computer systems that results in at least $1,000 aggregate damage; and the fraudulent trafficking in computer passwords affecting interstate commerce.

Perhaps the most famous application of this statute was **United States vs. Morris (Second Circuit, 1991)**, the 1989 prosecution of Robert Tappan Morris, a Cornell University graduate student who, on November 2, 1988, released a computer "worm" across the Internet computer network.

Despite the successful prosecution in the Morris case and several other famous computer crime prosecutions (including prosecutions of computer hackers of the Legion of Doom and Masters of Deception), problems continued with the statute. The most glaring was the omission of what was called malicious code – computer viruses that could alter, damage or destroy computerized information.

As a result, in 1992 Congress amended the computer crime statute to punish those who, without the knowledge and authorization of the "persons or entities who own or are responsible for" a computer, bring about the transmission of "a program, information, code or command to a computer or computer system" with the intent to cause damage to the computer or information in the computer or prevent the use of the system.

As well as punishing intentional conduct, the amended statute criminalizes those who act "with reckless disregard or a substantial and unjustifiable risk" of damage or loss and would create a civil cause of action to obtain compensatory damages or injunctive relief for "any person who suffers damage or loss by reason of a violation of the section."

In addition to protecting the data contained on computers, federal law also attempts to protect the integrity or confidentiality of electronic communications -- either during transmission or while stored. Section 2701 protects e-mail messages by making it illegal to destroy e-mail messages or access them without authorization.

In addition, in 1986 Congress amended the federal wiretap law, passing the Electronic Communications Privacy Act (ECPA) to expand federal jurisdiction and to criminalize the unauthorized "interception" of stored and transmitted electronic communications. The statute makes it unlawful to either intercept or disclose the contents of electronic communications, except as provided by statute. Thus, capturing or monitoring the contents of e-mail messages, electronic communications or stored electronic communications may violate these provisions.

The law does permit providers of telecommunications facilities to engage in some monitoring for the protection of those iacilities. In addition, the law allows monitoring if at least one of the parties to the monitoring has consented. Thus many companies use warning banners to notify users of their intent to monitor electronic mail, creating an implied consent.

The Justice Department's Computer Crime Unit, in conjunction with a number of federal agencies known as the Computer Search and Seizure Working Group, have developed guidelines to address seizing computers and handling computer evidence.

The guidelines run several hundred pages, addressing the many scenarios under which government officials could, in connection with criminal investigations, search or seize a company's (or a person's) computer data or equipment – including everything from computer hardware to e-mail messages.

4.8 EVOLVING PRECEDENTS

Where new laws have not kept up with the changing face of crime, authorities have used traditional statutes – mail and wire fraud, larceny, theft of services, embezzlement, trespass and destruction of property – to prosecute individuals who commit forms of computer abuse. Because these laws were not written with computer crimes in mind, courts must carve out new precedents.

Information: The application of common law concepts of fraud, theft and trespass were an ill fit to the new technology that emerged in the late 1960s. For example, the federal embezzlement statute (18 U.S.C. Section 641) proscribes the "conversion" or taking for one's own purposes of federal property. (There is no federal statute relating to the taking of commercial property). But it was unclear from the statute's inception whether information contained on a computer was truly property subject to conversion. The computer crime law of 1986, as already discussed, carved out certain circumstances under which the tampering with or taking of computer information would be a crime, but it did not establish a blanket protection for digitized information.

While some early cases, such as **Chappel vs. United States (Ninth Circuit, 1959)**, held that the embezzlement statute applies only to "corporeal or tangible property," most courts have ruled in the opposite direction. Convictions have been upheld for unauthorized use of computer time, theft of grand jury transcripts and photocopying government records.

In **United States vs. McAusland (Fourth Circuit, 1992)**, an employee was convicted of embezzlement for stealing a competitor's confidential bid information. The defendant, an employee of a defense contractor, obtained bid information by working with an employee at a competing company. The defendant was convicted of conspiracy to embezzle. While computer and computer information were not used in the crime, the case set the groundwork for determining whether information can be considered property.

Similarly, concepts of trespass and breaking and entering do not fit well into the electronic environment. There is no physical entry into the computer and therefore, no common-law trespass. Prosecutors have attempted to base charges on provisions of the wire fraud statutes, again with mixed results.

In **United States vs. Riggs (Northern District of Illinois, 1990)**, defendants Robert Riggs and Craig Niedorf, admitted computer hackers, devised what the district court accepted to be a scheme to steal software and other intellectual property belonging to Bell South. The data was designed to regulate the company's enhanced 911 (E911) emergency call system.

Riggs accessed the Bell South computer using other people's passwords and downloaded a text file that described the system. Though theoretically the pair could have been convicted under the wire fraud statute for stealing passwords, the two were never charged with this crime. Instead, the case concentrated on whether the information stolen could be considered property. The attorneys for the defense argued that the E911 data did not constitute property and that, therefore, no crime was committed.

In this instance, the court shared the prosecutor's view that the old law could be adapted to address the new crime. The district court, in denying the motion to dismiss the wire fraud count, observed: "... the object of the defendants' scheme was the E911 text file, which Bell South considered to be valuable, proprietary information. The law is clear that such valuable, confidential information is 'property,' the deprivation of which can form the basis of a wire fraud charge."

In another case, **United States vs. Brown (Tenth Circuit, 1991)**, the circuit court, also relying on Dowling, reversed the defendant's conviction for stealing a source code created by his former employer. The defendant had downloaded a copy of the source code onto his home computer, which was discovered later when a search was conducted in accordance with a warrant. This is not prosecutable under the Computer Fraud and Abuse Statute because it did not involve unauthorized entry. Dowling used his old password, which had not been purged from the computer system, to obtain the data.

In dismissing the indictment, the court observed that "Dowling holds that the statute applies only to physical goods, wares or merchandise. Purely intellectual property is not within this category. It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible."

While deprived of criminal remedies, companies can still pursue civil cases. The intent behind the law is to protect those that, for example, download copyrighted material to read later. It also makes these types of copying distinct from those taking material to resell it or gain other economic benefit.

A recent case typifies the problem of the enforcement of trade secrets in cyberspace.

In **Religious Technology Center vs. Netcom et al (Northern District of California, 1995),** the court declined to continue an injunction preventing the further publication of the trade secrets of the Church of Scientology.

One of the defendants in the case had obtained what the court concluded were secret internal documents of the church and had posted them on various Internet newsgroups. The defendant asserted that he had received some of the documents from various anonymous, publicly accessible Internet sites. The court concluded that information posted to the Internet could no longer be considered secret. Therefore, the individual who obtained the information from a public domain could not be held responsible for theft of trade secrets.

Further, the court ruled that "...evidence that another individual has put the alleged trade secrets into the public domain prevents the plaintiff from further enforcing its trade secret rights to those materials."

Another offense complicated by the nature of computers is the destruction of property. If an offender equipped with a sledge hammer pummels a computer into an unrecognizable pile of chips and wires, he or she has clearly committed the offense of destruction of property. If the same offender, equipped with a modem, deletes files from a computer system, all he or she has done is to change the polarity of a magnetic medium, which may or may not constitute a destruction of property.

While Congress attempted to address this concern with the Computer Fraud and Abuse law, it does not clearly define the concept of "loss." If information is stolen from a company, but the data still resides on the organization's computer system, it is unclear whether a loss has occurred.

The federal statute, rather than address destruction of property, addresses the concept of loss through unauthorized access, leaving open the question of whether computerized information is property and whether theft or deletion of the information is destruction of that property.

Companies may find their level of legal recourse for such destructive actions varies depending on the state in which the crime occurs. Texas, for example, adapted its legal code to criminalize unauthorized conduct that causes a computer to malfunction or that destroys or alters computer data.

In **Burleson vs. Texas (Texas Appeals Court, 1991)**, Burleson, a senior programmer, was fired. In retaliation, he inserted into the company's computer system a software program called a logic bomb. The program was designed to delete files responsible for calculating payroll commissions for more than 400 employees.

In this case, the crime was committed in a state that had brought its laws up to date. He was successfully prosecuted for violation of the Texas computer crime statute, passed in 1985 and updated in 1989, which makes it a crime for anyone to knowingly cause a computer to malfunction without the authorization of the owner or to alter, damage or destroy data or programs without the consent of the owner.

The court's ruling illustrates that the insertion of software devices designed to disable computer systems without the authorization of the owner may subject the perpetrator to both civil and criminal liability.

4.9 STATE STATUTES IN USA

On the state level, the one thing upon which there is much unanimity is that theft of information or money in electronic form is much the same as theft in any other form. State laws on computer crime, therefore, focus on theft of information or money through the use of a computer or an on-line computer service.

Virtually every state requires that one have the requisite mental state before they may be convicted of a computer crime. One must willfully, knowingly or purposely access computer-based data and intend to steal, destroy or alter computer-based information, steal services, passwords or otherwise interfere with hardware or software etc. It is not enough for purposes of these laws to accidently or unintentionally wander into areas on the internet where valuable or secure information may reside. If one enters such an area using computers or computer technology, his/her intent must be to steal, destroy or defraud to be found guilty of a crime.

Only a handful of states don't explicitly ban access to certain computer files. In most states mere access can be prosecuted as a crime. In addition, many states have the additional requirement that damage sustained by the victim of the crime be of a certain amount before the crime becomes a felony.

There are few states in USA which also have a statue regarding the Data alteration or source code theft, which are as follows[16]:

California: Penal Code 502 provides knowingly, willful for additional punitive or exemplary damages Access; introduce virus; traffic in providing access; theft of services valued under $400, fine up to $5000 or imprisonment in county jail for up to 1 year, for first offense that doesn't result in injury Access plus scheme to defraud; alter, damage or destroy hard/software valued over $5000; theft of services valued over $400; access and alters, destroys, uses, copies, damages data or disrupts computer services punishable by fine up to $10,000 or imprisonment in county jail for 1 year, for offense that results in injury or 2nd or subsequent offense.

Illinois: Section 720 1LCS 5/16D-1, et seq provides knowingly access or cause to be accessed, falsified e-mail information or other routing information in transmission of unsolicited bulk e-mail through e-mail service provider or its subscribers or gives software enabling this, class B misdemeanor; access and obtain data or services, class A misdemeanor for 1st offense Class 4 felony: access with purpose to scheme, defraud or deceive; damages computer or alter, delete or destroy program

[16] http://law.jrank.org/pages/11804/Computer-Crimes.html.htm

or data in connection with scheme, defraud or deceive; if offender accesses computer and obtains money or control of money in connection with his/her scheme, defraud or deception; class 3 felony if any of the above are 2nd or subsequent offense; class 4 felony: if value of money, property or services is $1,000 or less or if 2nd or subsequent offense obtaining data or services; class 3 felony: if value between $1,000 and $50,000; class 2 felony: if value $50,000 or more.

Nebraska: Section 28-1343, et seq. provides intentionally commission of unauthorized computer access in a manner that creates risk to public health/safety is class I misdemeanor; commission of unauthorized computer access in a manner that compromises the security of data is class II misdemeanor; unlawfully accessing computer to obtain confidential public info is class II misdemeanor; second or subsequent offense is a class I misdemeanor; accessing without authorization or exceeding authorization is class V misdemeanor; second or subsequent offense is class II Access with intent to deprive or obtain property/services is a class IV felony; if value of property/services is $1,000 or more, then class III felony; access and damage, disruption or distribution of destructive computer program, then class IV felony; if losses with a value of $1,000 or more, then class III felony; if causes grave risk of causing death, then class IV felony.

New Jersey: Section 2C:20-23, et seq.: Section does not specifically classify crimes listed as either felony or misdemeanor. Offenses listed in misdemeanor or felony columns are based on the levels of punishments imposed rather than by explicit classification. It provides purposely, knowingly Access; any of the following, causing damages less than $200: access plus scheme to defraud; alter, damage or destroy hard/software Access; any of the following, causing damages greater than $200: access plus scheme to defraud; alter, damage or destroy hard/software.

New mexico: Section 30-45-1, et seq. provides Knowingly, willfully Any of the following, causing damages less than $250: access; access plus scheme to defraud; alter, damage or destroy hard/software; disclosure, copy or display of computer information; less than $100 is a petty misdemeanor Any of the following, causing damages greater than $250: access; access plus scheme to defraud; alter, damage or destroy hard/software; disclosure, copy or display of computer information; $250 to $2500 in damages, 4th degree felony; $2500 to $20,000, 3rd degree felony, $20,000 or greater, 2nd degree felony.

North carolina: Section 14-453, et seq. provides willfully Class 1 misdemeanors: unlawful access of computers for purposes other than to scheme, defraud or obtain property; altering, damaging or destroying computer software, programs or data Class G felony: to access computer with purpose to scheme, defraud, obtain property; also Class G felony: to damage computer, computer system, computer network or parts thereof; Class F felony: access to any government computer; Class H felony: denying access to government computer services.

Oklahoma: Tit. 21, §§1951, et seq. provides Willfully Access or use of cause to be used computer services Access plus scheme to defraud; alter, damage or destroy hard/software; denial of access; traffic in passwords. There are several prohibited acts under the Computer Crimes Act classified as a felony.

Rhode island: Section 11-52-1, et seq. Provides Purposefully, intentionally; knowingly Theft of data or services valued under $500; cyber stalking Access of computer for fraudulent purposes; intentional access, alteration, damage or destruction; computer theft with a value over $500; use if false information and tampering with computer source documents.

South dakota: Section 43-43B-1, et seq. provides Knowingly Obtaining use, altering or destroying system, access and disclosure without consent where value is $1000 or less, class 1 misdemeanor; obtaining use, altering or destroying system

as part of deception where value involved is $1000 or less, class 1 misdemeanor Obtaining use, altering or destroying system, access and disclosure without consent where value involved is more than $1000, class 6 felony; Obtaining use, altering or destroying system as part of deception; value is more than $1000, class 4 felony.

Texas: Penal Code 33.01, et seq. provides Break of computer security is class B misdemeanor; class A if the amount involved is above $1,500 Break of computer security is a state of jail felony if amount involved is between $1,500 and $20,000 or amount is less than $1,500 and defendant has previous conviction; felony of third degree is amount between $20,000 and $100,000; felony of second degree if amount between $100,000 and $200,000; felony of first degree if amount is $200,000 or above.

Wisconsin: Section 943.70 provides Offenses against computer data and programs class; Offenses against computer data and programs is if offense is to defraud or obtain property, class I; if damage greater than $2500 or act causes interruption or impairment of govt. operations or public utility or service, class D; if offense creates risk of death or bodily harm to another, class F; offense against computer, computer equipment or supplies is class I if offense is done to defraud or obtain property; class H if damage is under $2500; and class F if act creates risk of death or bodily harm to another

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Explain the different ways of data alteration.

.....

.....

.....

.....

4.10 LEGAL POSITION IN INDIA

The Information Technology Act has added a new word, cyber crimes, which covers various kinds of computer and Internet related crimes.

As per the cyber crimes investigation cell, Mumbai provides the list of the cyber crimes which are as follows:

a) Hacking

b) Denial of Service Attack

c) Virus Dissemination

d) Software Piracy

e) Pornography

f) IRC Crime

g) Credit Card Fraud

h) Net Extortion

i) Phishing

j) Spoofing

k) Cyber Stalking

l) Cyber Defamation

m) Threatening

n) Salami

o) Sale of Illegal Articles

The real tangible threat of hacking comes in when an unauthorized access to a system is done with the intention of committing further crimes like fraud, misrepresentation, downloading data in order to commit infringement of copyright, accessing sensitive and top secret data from defence sites etc.

Trespass actions are grounded in the idea of protecting the owners control over real property, there is no inherent reason as to why the owners control over a websites could not be considered as species of property subject to trespass. It is for this reason that hacking is made a crime punishable under Section 66 (2) of the Information Technology Act, 2000 providing for an imprisonment up to 3 years or with fine up to Rs. 5 lacs or with both.

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

The offence of deliberately and malafidely destroying or altering the data bases of alien computers may best be described as 'Mischief' as defined in sections 425 to 440 of the Indian Penal Code. The essential ingredients for the offence of Mischief being

a) wrongful loss or damage to the public or any person

b) intention to cause such damage or knowledge that such damage or loss might be caused.

c) destruction of property or such alteration to such property as may render it useless or diminishes its value and/or utility.

d) Amply cover and describes the commission of the offence of destruction of digital data.

It has been mentioned that website could be considered to be the "property". Further, it cannot be denied that viruses, however harmless, cause damage to property to some extent. Thus the requirement of damage to property is met in the form of alteration or destruction of digital information through viruses.

The law dealing with Cyber crimes has now been codified in the I. T. Act, 2000 and Chapter XI deals with computer crimes and provide for punishments for these offences.

4.11 CASE STUDY

1) In July 2004, Microsoft hired an unnamed security company and a FBI agent to make a purchase on a site known as illmob.org, ran by William Genovese. The purchase revealed that Williams was distributing copies of the stolen source

code for Windows NT 4.0 and Windows 2000. One year later in August 2005 Genovese confessed to the illegal distribution and as a consequence was fined $250, 000 and sentenced to 10 years in prison. [2]Genovese claims that he had been singled out because FBI agents could not locate the criminals who actually stole the code which was originally 'hijacked from a comprised server owned by long time Microsoft partner Mainsoft Corporation' (The Register, October 15th). The leak and distribution of the Microsoft source code can and will cause many problems. Firstly, Microsoft may respond to this security scare by heavily reducing the number of employees who get to see the source code thus placing a larger work load on a selected few. Secondly and more notably this illegal practice has damaged the high level of security Microsoft provides. This is a problem because now that the source code is available malicious outsiders will use the source code and are also free to find bugs. As a result honest users will receive 'security drawbacks of open source without the security benefits'[17].

2) One day a young Software engineer came to State Cyber police office and complained that his web portal has been copied and being used in the other brand name. Cyber police asked him to demonstrate the same. The engineer opened his portal and the suspected portal and changed one of the source code of his image in the portal. It could be seen that the images on the suspected portal also changed. After verifying several similarities Cyber police found the claims of the engineer from Bhopal to be true.

   After preliminary investigation a FIR has been lodged against the owner of the suspected portal for copying the source code of the portal and using the same after making some changes for his use. During investigation the details about the site owner were obtained from the domain registry sites and profile of the suspect has been built up. The suspect has been found to be Australian of Indian origin[18].

3) **Oracle faces $100m source code theft lawsuit[19]**

   It has been reported that Oracle is facing a $100m (£63.9m) lawsuit after security software firm 2FA accused Oracle's subsidiary Passlogix of stealing source code for authentication and credential management.

   2FA claims the stolen code was used for Passlogix's v-Go software, which is being used by Oracle, although the alleged theft took place before Oracle took over Passlogix. "Oracle has been and continues to sell software misappropriated from 2FA, even after being notified by 2FA of its illegal actions," the security firm said in court documents. 2FA said agreement with Passlogix in 2006 provided licence to 2FA software "under very restrictive terms," according to Australian reports.

   The security firm has also alleged that a Passlogix product manager sent an e-mail containing 2FA source code to other members of staff who "had no requirement to access" such information. 2FA claims the damage caused by Passlogix's and Oracle's illegal actions is to be worth more than $10m, but the company is seeking over $100m, including punitive damages. 2FA claims Oracle knew or should have known, that some of the intellectual property it was acquiring in the Passlogix deal was illicitly taken.

---

[17] http://wiki.media-culture.org.au/index.php/Software_Piracy_-_Case_Studies_-_Theft_of_Microsoft_Source_Code

[18] http://mpcyberpolice.nic.in/casestudies.htm

[19] http://www.computerweekly.com/Articles/20110112244842Oracle-faces-100m-source-code-theft-lawsuit.htm.htm

Oracle won $1.3bn in damages from SAP for copyright infringement by its TomorrowNow subsidiary. Oracle filed that suit in 2007, claiming TomorrowNow illegally copied software code from Oracle systems needed to support customers, without buying licences to access it.

4.12 ONLINE DISPUTE RESOLUTION[20]

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

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

Defining Online Dispute Resolution

Dispute resolution techniques range from methods where parties have full control of the procedure, to methods where a third party is in control of both the process and the outcome. These primary methods of resolving disputes may be complemented with Information and Communication Technology (ICT). When the process is conducted mainly online it is referred to as ODR, i.e. to carry out most of the dispute resolution procedure online, including the initial filing, the neutral appointment, evidentiary processes or al hearings if needed, online discussions and even the rendering of binding settlements. Thus, ODR is a different medium to resolve disputes, from beginning to end, respecting due process principles.

ODR was born from the synergy between ADR and ICT, as a method for resolving disputes that were arising online and for which traditional means of dispute resolution were inefficient or unavailable. The introduction of ICT in dispute resolution is currently growing to the extent that the difference between off-line dispute resolution and ODR is blurry. It has been observed that it is only possible to distinguish between proceedings that rely heavily on online technology and proceedings that do not. Some commentators have defined ODR exclusively as the use of ADR assisted principally with ICT tools. Although part of the doctrine incorporates a broader approach including online litigation and other sui generis forms of dispute resolution when they are assisted largely by ICT tools designed ad hoc. The latter definition seems more appropriate since it incorporates all methods used to resolve disputes that are conducted mainly through the use of ICT. Moreover, this concept is more consistent with the fact that ODR was born from the distinction with off-line dispute resolution processes.

In ODR, the information management is not only carried out by physical persons but also by computers and software. The assistance of ICT has been named by Katsh and Rifkin as the 'fourth party' because ODR is seen as an independent input to the management of the dispute. In addition to the two (or more) disputants and the third neutral party, the labelling of technology as the fourth party is a clear

[20] http://en.wikipedia.org/wiki/Online_dispute_resolution

metaphor which stresses how technology can be as powerful as to change the traditional three side model. The fourth party embodies a range of capabilities in the same manner that the third party does. While the fourth party may at times take the place of the third party, i.e. automated negotiation, it will frequently be used by the third party as a tool for assisting the process.

The fourth party may do many things such as organize information, send automatic responses, shape writing communications in a more polite and constructive manner e.g. blocking foul language. In addition, it can monitor performance, schedule meetings, clarify interests and priorities and so on. The assistance of the fourth party will increase the more technology advances, thus reducing the role of the third neutral party. Katsh and Wing argue that ICT advance is occurring exponentially since ICT advance speeds up over the time. As a result, ODR processes are increasing in efficiency providing their disputants with greater advantages in terms of time saving and cost reductions.

Alternative definitions

In practice , it is difficult to provide a self-contained definition of ODR and given the pace of change it may not even be possible to do so. The use of technology usually involves the use of Internet-based communications technology at some stage, but ODR does not necessarily involve purely online processes – further, many could be replicated offline using pen and paper or could be achieved using computers without Internet connections.

The range of terms and acronyms used to describe the field augments the confusion often felt by those unfamiliar with the new field of ODR. These terms include:

- Internet Dispute Resolution (iDR)
- Electronic Dispute Resolution (eDR)
- Electronic ADR (eADR)
- Online ADR (oADR)

It is uncertain whether these processes form a new discipline of ADR or a tool to aid existing methods of dispute resolution. The most appropriate view would be to view ODR as an interdisciplinary field of dispute resolution.

ODR Methods[21]

- **Consensual Methods**

  Automated Negotiation: Automated Negotiation relates to those methods in which the technology takes over (aspects of) a negotiation. Most of the ODR services in this area are so-called 'blind-bidding' services. This is a negotiation process designed to determine economic settlements for claims in which liability is not challenged. There are two forms of automated negotiation, Double Blind Bidding, which is a method for single monetary issues between two parties and Visual Blind Bidding, which can be applied to negotiations with any number of parties and issues.

  Double Blind Bidding: Double Blind Bidding is a negotiation method for two parties where the offer and demand are kept hidden during the negotiation. It commences when one party invites the other to negotiate the amount of money in dispute. If the other party agrees, they start a blind bidding process whereby both parties make secret offers or bids, which will only be disclosed if both offers match certain standards.

[21] http://en.wikipedia.org/wiki/Online_dispute_resolution

Visual Blind Bidding: The primary distinction of Visual Blind Bidding is in what is kept hidden from the other parties. In traditional Double Blind Bidding, the offers and demands are kept hidden, whereas with Visual Blind Bidding what is kept hidden is what each party is willing to accept. This method can be effectively applied to the simplest single-value negotiations or the most complex negotiations between any number of parties and issues.

Visual Blind Bidding commences when all parties agree to negotiate with one another. They start the process by exchanging visible optimistic proposals, which define bargaining ranges. The system then generates suggestions that fall within the bargaining ranges. Parties may continue to exchange visible proposals or contribute their own suggestions to the mix. Suggestions contributed by the parties remain anonymous, thus avoiding the face saving problem of accepting a suggestion made by another party.

Thus, ODR is useful for resolving brick and mortar disputes that arise in businesses, insurance companies and municipalities, who are finding that ODR saves them money and time when dealing with B2C disputes.

Assisted Negotiation: In Assisted Negotiation the technology assists the negotiation process between the parties. The technology has a similar role as the mediator in mediation. The role of the technology may be to provide a certain process and/or to provide the parties with specific (evaluative) advice.

Mediators use information management skills encouraging parties to reach an amicable agreement by enabling them to communicate more effectively through the rephrasing of their arguments. Conciliation is similar to mediation, but the conciliator can propose solutions for the parties to consider before an agreement is reached. Also, assisted negotiation procedures are designed to improve parties' communications through the assistance of a third party or software. In fact, it has been argued that assisted negotiation, conciliation and even facilitation, are just different words for mediation. The major advantages of these processes, when used online, are their informality, simplicity and user friendliness.

- **Adjudicative Methods**

Online Arbitration: Arbitration is a process where a neutral third party (arbitrator) delivers a decision which is final and binding on both parties. It can be defined as a quasi-judicial procedure because the award replaces a judicial decision. However, in an arbitration procedure parties usually can choose the arbitrator and the basis on which the arbitrator makes the decision. Once the procedure is initiated parties cannot abandon it. Another feature of arbitration is that the award is enforceable almost everywhere due to the wide adoption of the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. Moreover, arbitral awards prove frequently easier to enforce than court decisions from overseas.

Although online arbitration seems admissible under the New York Convention and the E-Commerce Directive, this is arguably an assumption by most commentators, rather than a legal statement. Since arbitration is based on a contractual agreement between the parties, an online process without a regulatory framework may generate a significant number of challenges from consumers and other weaker parties if due process cannot be assured. The main challenge for online arbitration is that if judicial enforcement is required then it partly defeats the purpose of having an online process. Alternatively, some processes have developed self-enforcement mechanisms such as technical enforcements, black lists and trustmarks.

The Uniform Domain Names Dispute Resolution Policy (UDRP)

Traditionally, arbitration resolves disputes by delivering a decision that will be legally binding, i.e. enforceable by the courts in the same manner as a judgment. Non binding arbitration processes may also be effective when using ODR tools because they often encourage settlements by imparting a dose of reality and objectivity. In addition, self-enforcement measures may reinforce the efficacy of non binding processes.

The most significant example is the Uniform Domain Name Dispute Resolution Policy (UDRP) created by the Internet Corporation for Assigned Names and Numbers (ICANN). Some commentators have referred to the UDRP as an administrative process. In any case, the UDRP has developed a transparent global ODR process that allows trade mark owners to fight efficiently cybersquatting. The UDRP is used to resolve disputes between trade mark owners and those who have registered a domain name in bad faith for the purpose of reselling it for a profit or taking advantage of the reputation of a trademark.

Trademark owners accessing the UDRP must prove to the panel three circumstances:

1) similarity of the domain name to the trade or service mark;

2) lack of rights or legitimate interest in the registered domain name;

3) bad faith in the registration and use of the domain name.

However, the UDRP presents its own problems that show the challenges that an online adversarial system applied to mainstream e-commerce disputes would have. The main worry is that the evaluation of the panel decisions often shows a lack of unanimous consensus in the interpretation of the UDRP.

The UDRP providers have dealt efficiently with over 30,000 domain name disputes. Their success derives from two aspects: First, the UDRP deals only with blatant disputes, which are abusive registrations made in bad faith in order to take advantage of the reputation of existing trademarks. Secondly, it has incorporated a self-enforcement mechanism, which transfers and cancels domain names without the need for judicial involvement. This is a positive accomplishment for the development of e-commerce because it favours consumers' confidence in the Internet by reducing the number of fraudulent registered domain names.

Chargebacks: One of the main focuses of e-commerce up until recently has been related to secure payments. Chargebacks is a remedy used to reverse transactions made with credit or debit cards when a fraudulent use has occurred or when there is a violation of the contract terms. This method is very popular among online consumers since this is the main mechanism to transfer money online. In addition, consumers are not required to give evidence to cancel a payment. The vendor has the burden of proving that the merchandise or service was given according to the contract terms. Once this is proved the bank makes effective the payment to the vendor.

Chargebacks are largely used around the world by banks and the main credit card suppliers i.e. Visa, Mastercard and American Express.

ODR in the European Union

The European Small Claims Procedure: Small claims procedures provide a middle ground between formal litigation and ADR, where disputes involving small value claims can be resolved in courts faster, cheaply and less formally. The main limitation of small claims procedures is that they are restricted to particular jurisdictions. In order to overcome this limitation the European Commission has produced a regulation for a European Small Claims Procedure (ESCP).

Implementation of the ESCP is expected in all EC Member States by January 2009. The ESCP is predominantly a written procedure that deals with claims under 2,000 arising in cross-border disputes. Its main advantage is that it provides for the enforcement of decisions in any of the member states without the present need to go through the formal mutual recognition of judgements (exequatur).

Great expectations are put on the ESCP, which in order to deliver a cost effective process will have to rely on ICT. This will be a significant challenge, because unlike the UDRP, which is becoming a fully online process for dealing with specific complaints, the ESCP will deal with a variety of civil and commercial disputes. The objective of the ESCP is the creation of a cost efficient procedure applicable to small value claims in cross-border disputes. This objective could only be achieved by using a written procedure, assisted by electronic forms such as e-mails and videoconferencing as foreseen by the ESCP.

The Regulation allows the use of new technologies in transferring information and evidence between the courts of the different member states. But, it will be the EC Member States who will decide, through their own regulations, which specific means of communication are acceptable in their courts. Given that the ESCP is a regulation and not a directive, it is arguable whether it has left too many aspects to the discretion of member states, which could call into question the legal certainty expected from a European regulation. Nevertheless, it can be expected that, in due time, electronic communications will reach every possible and reasonable aspect of the judicial procedure to assist in the resolution of online as well as off-line B2C disputes.

It is expected that the ESCP will contribute to mitigate the legitimacy problem which also hampers the emergence of ODR. Perhaps, within the EU, where we have concern for the fairness of private procedures (i.e. restrictions in consumer arbitration) the ESCP may contribute to increase trust in ODR processes.

ODR in India

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

ODR Clause

Example of Tiered ODR clause: If a dispute arises out of or relates to this Agreement or the breach thereof and if the dispute cannot be settled through negotiation, the parties agree first to try in good faith to settle the dispute by online mediation [or alternatively, insert another consensual method of Online Dispute Resolution (ODR)] administered by [Insert forum]. If the parties do not reach a voluntary settlement through such ODR procedure within a period of [30] days or the period

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Define ODR?

.....

.....

.....

.....

2) Explain ODR Methods.

.....

.....

.....

.....

4.13 LET US SUM UP

This unit deals with important discussion on the possibility of data alteration and destruction and theft. This unit discusses the ways or mechanism of such alteration and the ways for preventing the same.

4.14 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

money in dispute. If the other party agrees, they start a blind bidding process whereby both parties make secret offers or bids, which will only be disclosed if both offers match certain standards.

Visual Blind Bidding: The primary distinction of Visual Blind Bidding is in what is kept hidden from the other parties. In traditional Double Blind Bidding, the offers and demands are kept hidden, whereas with Visual Blind Bidding what is kept hidden is what each party is willing to accept. This method can be effectively applied to the simplest single-value negotiations or the most complex negotiations between any number of parties and issues.

Visual Blind Bidding commences when all parties agree to negotiate with one another. They start the process by exchanging visible optimistic proposals, which define bargaining ranges. The system then generates suggestions that fall within the bargaining ranges. Parties may continue to exchange visible proposals or contribute their own suggestions to the mix. Suggestions contributed by the parties remain anonymous, thus avoiding the face saving problem of accepting a suggestion made by another party.

Thus, ODR is useful for resolving brick and mortar disputes that arise in businesses, insurance companies and municipalities, who are finding that ODR saves them money and time when dealing with B2C disputes.

Assisted Negotiation: In Assisted Negotiation the technology assists the negotiation process between the parties. The technology has a similar role as the mediator in mediation. The role of the technology may be to provide a certain process and/or to provide the parties with specific (evaluative) advice.

Mediators use information management skills encouraging parties to reach an amicable agreement by enabling them to communicate more effectively through the rephrasing of their arguments. Conciliation is similar to mediation, but the conciliator can propose solutions for the parties to consider before an agreement is reached. Also, assisted negotiation procedures are designed to improve parties' communications through the assistance of a third party or software. In fact, it has been argued that assisted negotiation, conciliation and even facilitation, are just different words for mediation. The major advantages of these processes, when used online, are their informality, simplicity and user friendliness.

Adjudicative Methods

Online Arbitration: Arbitration is a process where a neutral third party (arbitrator) delivers a decision which is final and binding on both parties. It can be defined as a quasi-judicial procedure because the award replaces a judicial decision. However, in an arbitration procedure parties usually can choose the arbitrator and the basis on which the arbitrator makes the decision. Once the procedure is initiated parties cannot abandon it. Another feature of arbitration is that the award is enforceable almost everywhere due to the wide adoption of the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. Moreover, arbitral awards prove frequently easier to enforce than court decisions from overseas.

Although online arbitration seems admissible under the New York Convention and the E-Commerce Directive, this is arguably an assumption by most commentators, rather than a legal statement. Since arbitration is based on a contractual agreement between the parties, an online process without a regulatory framework may generate a significant number of challenges from consumers and other weaker parties if due process cannot be assured. The main challenge for online arbitration is that if judicial enforcement is required then it partly defeats the purpose of having an online process. Alternatively,

some processes have developed self-enforcement mechanisms such as technical enforcements, black lists and trustmarks.

MPDD/IGNOU/P.O.1T/Oct.2011

ISBN: 978-81-266-5725-4