CYBER CRIMES: LAW AND PRACTICE*

Cyber crime means any criminal activity *i*n which a computer or network is the source, tool or target or place of crime. The Cambridge English Dictionary defines cyber crimes as crimes committed with the use of computers or relating to computers, especially through internet. Crimes involving use of information or usage of electronic means in furtherance of crime are covered under the scope of cyber crime. Cyber Crimes may be committed against persons, property and government. The common types of cyber crimes may be discussed under the following heads.

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

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

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

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

2. Cyber Stalking - This crime involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.

3. Spamming - Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates .negative impact on consumer attitudes towards Internet Service Provider.

4. Cyber Pornography - Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such funs. Later they are sexually exploited for gains.

5. **Phishing** - It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

6. Software Piracy - It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies.

---

* Prepared by Dr.A. Prasanna, Associate Fellow IMG ,Thiruvananthapuram.

7. Corporate Espionage - It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.

8. Money Laundering - It means moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. eg. Transport cash to a country having less stringent banking regulations and move it back by way of loans the interest of which can re deducted from his taxes. This is possible prior to computer and internet technology, electronic transfers have made it easier and more successful.

9. Embezzlement - Unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offender's care, custody or control is called embezzlement. Internet facilities are misused to commit this crime.

10. Password Sniffers - Password sniffers are programmes that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.

11. Spoofing - It is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted. Spoofing was used to access valuable information stored in a computer belonging to security expert *Tsutomu Shimomura.*

12. Credit Card Fraud - In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases.

13. Web Jacking - The term refers to forceful taking of control of a web site by cracking the password.

14. Cyber terrorism - The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country.

THE INFORMATION TECHNOLOGY ACT 2000

In India the Information Technology Act 2000 was passed to provide legal recognition for transactions carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital Property, and Digital Rights Any violation of these laws constitutes a crime. The Act prescribes very high punishments for such crimes. The Information Technology (amendment) Act, 2008(Act 10 of 2009) , has further enhanced the punishments. Life imprisonment and fine upto rupees ten lakhs may be given for certain classes of cyber crimes. Compensation up to rupees five crores can be given to affected persons if damage is done to the computer, computer system or computer network by the introduction of virus, denial of services etc.(**S. 46(1-A)).** Sections **65-74** the Act specifically deal with certain offences, which can be called Cyber Crimes

1. Tampering with any computer source code used for a computer, computer programme, computer system or computer network, is punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. "Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.(**S.65**)

2. Hacking with computer system is to be punished with imprisonment up to three years, or with fine which may extend up to five lakh rupees, or with both.(**S. 66)**

3. Sending offensive or false information through computer or a communicative device is punishable with imprisonment up to three years and with fine.(S.66A)

4. Receiving or retaining stolen computer resource or communication device is an offence punishable with imprisonment up to three years and fine up to one lakh or with both. (S.66B).The same punishment is prescribed for fraudulent use of electronic signature, password etc. of any other person (S. 66C) and for cheating using computer, cell phone etc. (S.66D)

5. Capturing Transmitting or publishing the image of a private area of any person without consent is punishable with imprisonment up to three years and with fine up to two lakhs or with both.(S. 66E)

6 Punishment for Cyber terrorism may extend to imprisonment for life. (S.66F)

7. Publishing transmitting information which is obscene in electronic form. shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.(**S. 67).**

8 Publication and transmission of containing sexually explicit act or conduct is to be punished with imprisonment up to five years and fine up to ten lakh rupees and for second or subsequent conviction with imprisonment for a term up to seven years and fine up to ten lakh rupees.(S. 67A) The same punishment is prescribed for child pornography. (S. 67B)

9. Penalty for Misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be. Shall be punished with imprisonment for a term, which may extend to two years, or with fine which may extend to one lakh rupees, or with both. **(S. 71)**

10. Penalty for Breach of Confidentiality and Privacy

Any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.(**S. 72)**

11. Punishment for disclosure of information in breach of contract is imprisonment For a term up to three years or with fine up to five lakh rupees or with both.(S. 72A)

12. Punishment for publishing Digital Signature Certificate false in certain particulars. (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any

other person with the knowledge that (a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

Violation of the above provision is punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. **(S. 73)**

13. Publication for Fraudulent Purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.(**S. 74.)**

In addition to the prescribed punishments Any computer, computer system, floppies, compact disks, tape drives or any other accessories related to the crime shall be liable to confiscation.(**S. 76**.) S. 75of the Act makes it clear that the provisions of this Act are applicable to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

* * *

Cyber Crimes- Indian Cases*

1. Pune Citibank Mphasis Call Center Fraud

It is a case of sourcing engineering. US $ 3,50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situations.. Later they used these numbers to commit fraud. Highest security prevails in the call centers in India as they know that they will lose their business. The call center employees are checked when they go in and out so they can not copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

2. State of Tamil Nadu Vs Suhas Katti

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits. The court relied upon the expert witnesses and other evidence produced before it, including witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved and convicted the accused. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India.

3.The Bank NSP Case

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

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

In this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from sending derogatory emails to the plaintiff. The plaintiff contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature and the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world.

The Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs. This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an injunction restraining the defendant from defaming the plaintiffs by sending defamatory emails.

5. Parliament Attack Case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

6. Andhra Pradesh Tax Case

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

7. Sony.Sambandh.Com Case

A complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients.

In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim .The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case. 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. The court convicted Arif Azim for cheating under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cyber crime 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 cyber crime 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. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

8. Nasscom v. Ajay Sood & Others - The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association.

The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The High court recognised the trademark rights of the plaintiff and passed an injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom. The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court. It became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks. The Delhi HC 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 misused." The court held that, to the consumer but even to the person whose name, identity or password is act of phishing as passing off and tarnishing the plaintiff's image.

This case achieves clear milestones: It brings the act of "phishing" into the ambit of India laws even in the absence of specific legislation; It clears the misconception that there is no" damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

---

*Source: http://delhicourts.nic.in/ejournals/CYBER%20LAW.pdf