WORLD AROUND TECHNOLOGY- CYBER LAWS IN THE 21ST CENTURY

Neha Sharma

University of Petroleum & Energy Studies, Dehradun

Definitions

Cyber Crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. -By Jennifer Williams U.S Government Criminal Law

Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:

Advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software;

Cyber-enabled crime – many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even Terrorism.

The Changing Nature of Cybercrime

"New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging."[1]

INTERPOL's Role

INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled crimes. Most cybercrimes are transnational in nature; therefore, INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local

[1] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

law enforcement with focused cyber intelligence, derived from combining inputs on a global scale."[2]

Types of Cyber Crimes

HACKING | The act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed. Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user.

DENIAL OF SERVICE ATTACK | This is an act by the criminal, who floods the band width of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

VIRUS DISSEMINATION | Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious soft wares)

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. It can be done in various ways such as end user copying, hard disk loading, Counterfeiting, Illegal downloads from the internet etc.

PORNOGRAPHY | Pornography is the first consistently successful ecommerce; product. It was a deceptive marketing tactics and mouse trapping technologies. Pornography encourage customers to access their websites. Anybody including children can log on to the internet and access website with pornography contents with a click of a mouse.

IRC CRIME | Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other Criminals use it for meeting co-conspirators. Hackers use it for discussing their exploits / sharing the techniques. Paedophiles use chat rooms to allure small children.

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 these cards by impersonating the credit card owner.

NET EXTORTION | Copying the company's confidential data in order to extort said company for huge amount.

[2] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

PHISHING | It is a technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means.

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 emails, entering the chat rooms frequently.

CYBER DEFAMATION | The Criminal sends emails containing defamatory matters to all concerned of 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 email 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 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."[3]

Cyber Crimes and the Law

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cybercrimes at the domestic and international level as well. "There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology "INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008]"[4]

[3] http://cybercrimes09.blogspot.in/2009/10/types-of-cybercrime.html
[4]http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

The Major Acts, which got amended after enactment of ITA

The Indian Penal Code, 1860

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

The Indian Evidence Act 1872

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the Act.

The Bankers' Book of Evidence (BBE) Act 1891

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data ...to retrieve data that is lost due to systemic failure or .... The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided, such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

Issues not covered under ITA

ITA and ITAA is though landmark first step and became mile-stone in the technological growth of the nation; however, the existing law is not sufficed. Many issues in Cybercrime and many crimes are still left uncovered.

Territorial Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cybercrime etc. Since cybercrimes are basically computer based crimes and therefore if the mail of someone is hacked in one place by accused sitting far in another state, determination of concerned P.S., who will take cognizance is difficult. It is seen that the investigators generally try to avoid accepting such complaints on the grounds of jurisdiction. Since the cybercrime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdictions; it is needed to proper training is to be given to all concerned players in the field. Preservation of evidence is also big issue. It is obvious that while filing cases under IT Act, very often, chances to destroy the necessary easily as evidences may lie in some system like the intermediaries' computers or sometimes in the opponent's computer system too.

However, most of the cybercrimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

Home Minister Rajnath Singh has said in Parliament recently that there was a need to strengthen cyber monitoring in the wake of growing use of Internet and social media by global terror outfits like ISIS to indoctrinate the youth.

Cyber Crimes

Distributed Denial of Service Attacks

A denial-of-service attack or Distributed Denial or Service (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically—but not exclusively—target sites or services hosted on high-profile web servers. Denial of service attacks are one form of computer sabotage whereby people can effectively ruin their target's operations for what could be a lengthy period of time.[5]

[5] http://www.newworldencyclopedia.org/entry/Cybercrime#Credits

Internet Auction Fraud

Online auctions have transpired into a very lucrative business. Many are making a living at buying/selling through online auction houses. Millions of online auction items are up for bid daily and include items from all around the world. This phenomenon keeps growing daily as more buyers and sellers flock to these online auction houses. This activity is offering great opportunities for buyers and sellers. Sellers are able to have their posted item viewed by millions of people and buyers are able to purchase hard to find items and/or items at discounted prices. However, these online auctions are also giving perpetrators another avenue to perpetrate fraud. Internet auction fraud is currently the number one fraud committed over the Internet. The Internet Fraud Complaint Centre (IFCC) lists auction fraud entailing 64% of more than 30,000 complaints received.[6]

Pay-Per Click Fraud

Click fraud (sometimes called pay-per-click fraud) is the practice of artificially inflating traffic statistics to defraud advertisers or Web sites that provide venues for advertisers. In the common pay-per-click advertising model, advertisers pay a fee for each click on their link. According to a CNET News article some industry segments have costs-per-click of several dollars. By using automated clicking programs (called hit bots) or employing low-cost workers to click the links, the perpetrators create the illusion that a large number of potential customers are clicking the advertiser's links, when in fact there is no likelihood that any of the clicks will lead to profit for the advertiser.

Click fraud scammers often take advantage of the affiliate programs offered by some Web sites, such as Google and Yahoo! Search Marketing. The scammers sign up for the affiliate programs, agreeing to provide further exposure to the advertising in question and receiving a portion of the pay-per-click fees in return. The perpetrators place the ads on Web sites created solely for this purpose that, naturally, don't have any real traffic. Once the ads are in place, the hitbots or workers generate large volumes of fraudulent clicks, often in a very short time period, for which the scammer bills the owner of the affiliate program. Both Google and Yahoo! Search Marketing have had to reimburse advertisers for pay-per-click fees that were discovered to have been the result of click fraud.[7]

Nigerian Advance Fee Fraud

Nick named as the 419 fraud, it is very familiar fraud to most us who are avid Internet users. Here the fraudster starts his operations with a letter something like below. It is estimated that more than 15 business men have been kidnapped and killed as a part of AFF scam in Nigeria. In fact, I have received a similar mail even on 23rd June 2009.

[6] http://www.cbintel.com/AuctionFraudReport.pdf
[7] http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci1000478,00.html

Reshipping Fraud

This scam is everywhere. Some advertisements are placed in newspapers, and you can even find listings on CareerBuilder.com as well as other job placement websites. When you answer the ad, the reshipping "employer" will ask that you send your personal information such as your social security number and date of birth. After the employer receives your information, packages will start arriving at your house with instructions on how to repackage and then ship the goods to addresses abroad.

When your payment for services performed arrives, it will be in the form of a third party cashier's check. This should raise red flags on your part since the accepted way of doing business is with a paycheck. These cashier's checks will usually be greater than the initially agreed amount. Then the employer will ask that you send back electronically what was overpaid to you. The moment you have completed this transaction, another problem arises. The bank will discover that the cashier's check was fake and hold you responsible for the full amount of the check. In addition, your "employer" has your personal information which will be used to defraud more unsuspecting people who become "employees" of this illegal money making scheme. You, the re-shipper, can get into big trouble because all the goods that you shipped overseas was bought with stolen credit cards. [8]

Diploma Scam

Quick degree scams - "Get your degree in 30 days!" "No studying required", "Turn your experience into a degree". They say they are accredited and the degree is legal and meaningful. That's part of the scam and when the scam is exposed that you purchased your degree; you'll be out on the street and no one will hire you. You may make the cover of a newspaper, exposed as the worthless hack you are for attempting to buy your degree. You may make a list of people who have purchased scam degrees that we're working on right now.[9]

Warez

"Warez" (pronounced "wearzz," NOT "wahr-ez") are pirated copies of proprietary commercial software, typically distributed over the Internet after the program's copyright protection mechanisms (if any) have been disabled. Pirated music, pirated movies and pirated games may also be distributed.

Case Law on Point

Insulting Images of Warrior Shivaji on Google - Orkut[10]

[8] http://ezinearticles.com/?Reshipping-Fraud---A-Home-Business-Con&id=582426
[9] http://www.consumerfraudreporting.org/Education_Degree_Scams.php
[10] Links to the following case studies on Cyber Crime were provided by Mr. Jay Srinivasan Head, Governance & Assurance, Fidelity India

An Indian posts 'insulting images' of respected warrior-saint Shivaji on Google's Orkut. Indian police come knocking at Google's gilded door demanding the IP address (IP uniquely identifies every computer in the world) which is the source of this negative image. Google, India hands over the IP address. No such incident in India would be complete without a few administrative slip-ups. The computer with that IP address is using Airtel, India as the ISP to connect to the internet and Orkut. Airtel gives police the name of an innocent person using a different IP address. How two IP addresses could be mixed-up in a sensitive police case is anyone's guess. An innocent Indian, Lakshmana Kailash K, is arrested in Bangalore and thrown in jail for 3 weeks. Eventually, his innocence is proved and he is released in Oct, 2007. A number of news media report this incident. American citizen and India lover Christopher Soghoian (home page http://www.dubfire.net/chris/) studies Informatics at Indiana University and researches/writes about security, privacy and computer crime. Christopher does an excellent article on this topic for the blogs at respected tech media group CNET. Like all good writers, Christopher Soghoian, gives Google, India a list of questions so that he can give a balanced perspective to the millions of CNET readers.

How does Google, India respond?

The only comment was: "Google has very high standards for user privacy and a clear privacy policy, and authorities are required to follow legal process to get information. In compliance with Indian legal process, we provided Indian law enforcement authorities with IP address information of an Orkut user."

How does it Airtel react to rectify its mistake?

Firstly, with an immediate, unqualified apology. In itself, a positive first step.

Techgoss (techgoss.com) had heard rumours about Airtel also offering monetary compensation to the person wrongly jailed. But Airtel is being coy about possible financial compensation. An Airtel spokesperson issued the following statement to techgoss.com

"Airtel are aware of this incident and deeply distressed by the severe inconvenience caused to the customer. We are fully cooperating with the authorities to provide all information in this regard and we are in touch with the customer. We have robust internal processes, which we review frequently to make them more stringent. We have conducted a thorough investigation of the matter and will take appropriate action".

What is the current Scenario?

Finally, he has demanded that he be compensated for the injustice meted out to him! The illegally accused and detained techie in the Chatrapati Sivaji defamation picture case on Orkut, Lakshmana Kailas K, has slapped a ten- page legal notice on Telecom giant Bharti Airtel, the Principal Secretary (Home) of the state government in Maharashtra, India and the Assistant Commissioner of Police (Financial & Cybercrime unit) demanding that an amount of 20 crores be paid as damages.

Some Recent Cases in India

Financial Crimes[11]

Wipro Spectramind lost the telemarketing contract from Capital one due to an organized crime. The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario.

Cyber Pornography

Some more Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face.

Online Gambling

Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound. After confirmation a telgu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

Intellectual Property Crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cybersquatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.

[11] Following case studies on Cyber Crime were provided by Dr. Uma Somayajula, an eminent IT Security professional and DSCI member

Cyber Stalking

Ritu Kohli has the dubious distinction of being the first lady to register the cyber stalking case. A friend of her husband gave her telephonic number in the general chat room. The general chatting facility is provided by some websites like MIRC and ICQ. Where person can easily chat without disclosing his true identity. The friend of husband also encouraged this chatters to speak in slang language to Ms. Kohli.

PR Theft | Jun 23, 2009 at 0119 hrs IST

The economic offences wing (EOW) of the Pune police on Monday arrested a software engineer Asma Sandip Thorve (37), a resident of Uday Society in Sahkar Nagar, for allegedly cheating Brainvisa Technologies to the tune of Rs 46.5 crores, by stealing their source code. Earlier, the police had arrested software engineer Sameer Ashok Inamdar (36) of Kondhwa in the same case. According to the police, Inamdar resigned from Brainvisa Technologies in August 2006. He allegedly stole the source code and other secret information of Brainvisa Technologies and started his own company. Owner of Brainvisa Technologies Nitin Hemchandra Agarwal had lodged a police complaint alleging that the company lost Rs 46.5 crores due to this. A team, led by assistant commissioner Pushpa Deshmukh, arrested Thorve, who was Inamdar's business partner and allegedly provided him the confidential data of Brainvisa. Thorve worked as senior manager, business development, for Brainvisa from May 2004 to December 2005 and there on as vice president till December 2008, after which she joined Inamdar as a partner. Thorve was produced before court on Monday and has been remanded to police custody till June 26.

Email Bombing (DoS)

In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data Diddling

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Credit Card Frauds

Amit Tiwari had many names, bank accounts and clients. None of them were for real. With a plan that was both ingenious and naïve, the 21-year-old engineering student from

Pune tried to defraud a Mumbai-based credit card processing company, CC Avenue, of nearly Rs 900,000.He was arrested by the Mumbai Police on August 21, 2003 after nearly an year of hide and seek with CC Avenue. He's been charged for cheating under Section 420.

India's First ATM Card Fraud

The Chennai City Police have busted an international gang involved in cybercrime, with the arrest of Deepak Prem Manwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt. The dimensions of the city cops' achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States. At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai.

Case of Cyber Extortion

He does not know much about computer hacking, yet 51-year-old cyber criminal Pranab Mitra has stunned even the cyber crime investigation cell of Mumbai police with his bizarre fraud on the Net. Mitra, a former executive of Gujarat Ambuja Cement, was arrested on Monday for posing as a woman and seducing online an Abu Dhabi-based man, thereby managing to extort Rs 96 lakh from him. Investigating officer, Assistant Commissioner of Police, J.S. Sodi, said Mitra has been remanded to police custody till June 24, and has been booked for cheating, impersonation, blackmail and extortion under sections 420, 465, 467, 471, 474 of the IPC, read with the newly formed Information Technology Act.

Reliance made to pay the Consumer

After conducting its own audit, Capital One, located in McLean, Virginia, rescinded the contract with Wipro in March. But its misadventure--and other recent departures from India by U.S. clients--has confirmed many doubts and concerns about the booming business of outsourcing call centers, and also is serving as a catalyst for human resources to develop more effective approaches to managing offshore workers. Experts and consultants believe that companies can meet the challenges and save millions of dollars by improving training and implementing tighter oversight of offshore call agents. Some U.S. companies have even installed their own teams at offshore call centres. "Capital One represents some of the challenges of outsourcing.

CONCLUSION

Computer crime is a multi-billion dollar problem. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cybercrime is a menace that has to be tackled effectively not only by the official but also by the users by co-operating with the law. The founding fathers of internet wanted it to be a boon to the whole world and it is upon us to keep this tool of modernisation as a boon and not make it a bane to the society.