LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

CYBER CRIME: THE NEW SPECIES OF CRIME *

Introduction

Now a days with the advent of industrialization and the fast development of the economy most of the human activities tend to depend more and more on technology, especially information technology. It goes without saying that humans are a superior form of life on earth and hence strive to achieve their goals by whatever means possible both lawfully and unlawfully. Information technology is one such example of the extent to which humans can go in order to fulfill their thirst for power.

What the developers of the World Wide Web and other information technologies didn't anticipate was, with the evolution of Internet comes another revolution of crime. In today's world cyber criminals do not require any considerable amount of technical knowledge, or even for a matter own a computer. All the information is wide open with minimal amount of security hence enabling the fast pace progress of cybercrime rates globally.

According to the Information Technology Act, 2008, cyber-crime is defined as an unlawful act committed using a computer either as a tool or as a target (or both) for facilitating a crime. Although in the definition there is an overlap, the most likely scenario is one use the computer as a tool, and the other use it as a target.

In order to understand cyber-crimes it is first and foremost necessary to understand that the computer itself does not commit the crime but people do. Cyber-crime is a result of misuse, destruction and corruption of technology which was made with the intention to benefit and simplify human life.

Totally denying oneself the use of technology is not the appropriate solution for cybercrime. These technologies have been developed for the comfort of its users and hence should be continued to be used for this purpose.

* M.Prakriti & G. Keerthna, 2nd Year, B.B.A LL.B (Hons.) Saveetha School of Law, Saveetha University.

Making of written laws and infrastructure for their enforcement and management alone is not sufficient to achieve the goal of clearing cyberspace or even any legal control regime. With experience comes great knowledge. The information that is derived while monitoring the actual working of the system is vital for improving the working of any system. Examples of cyber-crime include identity theft, transaction fraud, advance fee fraud, hacking, piracy, phishing, spamming, etc. With the tremendous growth and advancement of technology it's becoming more and more vital to have a system for continuous monitoring and evaluation of cyber-crime.

As of now there is no permanent remedy for cyber-crimes. There are certain laws made in efforts to reduce these crimes but no prominent solution as such. This essay deals with the legal aspects related to cyber space and crimes that are prevailing with respect to the Indian scenario.

CYBER SPACE: A NECESSARY EVIL

When mankind was introduced to information technology and cyber space they never anticipated what awaits them in the future. These comforts came to them at a cost, at the cost of their privacy. Nobody ever foresaw that one day the development of these communication and data transferring devices can become a curse for the people.

Now a days people with intelligence have found numerous ways to misuse the aspect of anonymity of the internet to perpetuate illegal activities in cyber space.

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.[1]

In earlier days, there was hardly any serious damage possible by any disgruntled employee but in today's computerized offices, angry workers and disgruntled employees can access computer systems and destroy data with a click of the mouse, causing millions of dollars in damage. A new type of cybercrime is emerging these days in which hackers demand money in return for not damaging the recipient's computer. We may call it extortion in cyberspace or "cyber extortion". People have been receiving e-mail threats that either to place the equivalent of $20 or $30 in a

[1] Internet crime, last visited April 15, 2016; http://www.cyberlawsindia.net/internet-crime.html

specific online bank account or they risk having vital computer files deleted from their office systems or having child pornography images added. It is technically possible for a hacker to send unwanted pictures into someone else's computer. But the strength of this scam is that the blackmailer merely has to make a credible threat. The small amount of money demanded also helps convince the victim to pay instead of taking the risk of losing important data or reputation.[2]

The internet with its timely development, continuous increasing speed and expansion of global access has created a bigger and better platform for the commitment of such cyber-crimes. Vivek Sood in his book broadly stated, 'cyber-crime'can be said to be an act of commission or omission, committed on or through or with the help of or connected with, the internet, whether directly or indirectly, which is prohibition by any law and for which punishment, monetary and/or corporal, is provided.[3]

Cyber-crimes can occur unnoticed, undetected and unreported as it is anonymous in nature. There are several mechanisms that facilitate anonymity, encryption being the most common method. "Encryption has become an essential part of doing business on the internet for companies and consumers alike. And the raising use of encryption technology has long been a concern of the FBI which has said that the technology can be devastating to criminal investigations."[4]

CYBER CRIME CASE REPORTED IN INDIA

The first ever report cyber-crime case was the Amit Vikram Tiwari case which was filed in the year 2003 and was again reported in the year 2014 as well.

In the year 2003 Indian law enforcement had some celebration to do. The Central Bureau of Investigation (CBI), essentially the country's version of the FBI, had caught its first ever cyber-criminal.

Amit Vikram Tiwari from Pune was allegedly the owner of two hacker-for-hire websites, www.hirehacket.net and www.anonymiti.com, which offer services for breaking into email accounts for the reasonable price range of $250 - $500. Before being arrested and the websites going offline, he reportedly hacked into more than 1,000 different accounts, to do everything from stealing funds to checking on the communications of families to potentially wed their sons and daughters to.

[2] DAVID INCOVE, A COMPUTER CRIME- A CRIME FIGHTER HANDBOOK, 29 (1955)
[3] VIVEK SOOD, CYBER LAW SIMPLIFIED, 39 (2001)
[4] JOHN SCHWARTZ, ORGANISED CRIME RAISES PRIVACY ISSUES, THE NEW YORK TIMES, 20 JULY 2001

He was "[...] a member of a full fledged organised and coordinated hacking network which spreads across many countries", according to CBI sources, who claimed that his international empire involves dealing with over $600 million. Additional raids in Mumbai, Pune and Ghaziabad have taken place to catch others.

However, before the country starts flaunting this as a major victory and rubbing it in the face of their Pakistani rivals, the Indian authorities cannot take all of the credit. In fact, most of it is owed to the American FBI, who, after investigating the sites based on U.S. servers, tipped off their Indian colleagues with Tiwari's GPS location.

Rather more embarrassingly—both for Indian law enforcement and the hacker himself—it appears that Tiwari was already known to the Mumbai police force. In 2003 he successfully obtained Rs. 900,000 ($14,300) by hacking a credit card processing company, and it looks like he was also approached to participate in an attack involving the Indian Premier League (IPL) , in which bookies sought information from the accounts of people involved in the competition.

Foolishly, Tiwar accepted most of his payments through Paypal and even Western Union Money Transfer. For someone who describes themselves as a professional hacker, use of Bitcoin or another crypto-currency never factored into his security protocol.

But putting aside the Indian police's negligence and Tiwari's egregious methods, perhaps this dependence on the American intelligence services won't last for much longer. Last June, India launched its own web of surveillance, that will "give its security agencies and even income tax officials the ability to tap directly into e-mails and phone calls", all without parliamentary or court oversight. After it is fully rolled out, the system will be able to specifically target any of India's 900 million phone lines and 120 million internet users, all in an apparent push to stifle terrorist plots.

Of course, at a time where privacy is one of the most pertinent issues in everyone's mind, there are worries that this snooping apparatus will affect the human rights of Indian citizens. It is also unclear whether such a system will actually be effective at catching criminals like Tiwari. For instance, the FBI tip only came about because Tiwari was stupid enough to host his websites on U.S. servers, which, in a post-Snowden world, are notoriously insecure.

As business in Silicon Valley and the U.S. tech industry in general diminishes due to concerns over backdoors and law enforcement collaboration, criminals may decide to host their nefarious

activities elsewhere. If Tiwari had done that in the first place, perhaps he wouldn't have been caught.[5]

COMPUTER RELATED OFFENCES

The internet is a very cheap and fast means of international communication of text, sound, video and image. The internet, in other words can be called and information resource free from any political or content boundaries, limited only by the extent to which the information providers are willing to disclose their material and the fruits of their work.

These features have led the users of the internet to have a false sense of freedom in their communication. While enjoying the benefits of information technology it's users fail to look out for the evils that can be done by means of the same technology.

A few computer related offenses have been noted below:

Pornography:

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional.

The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive.

Section 67 of the IT Act is the most serious Indian law penalizing cyber pornography. Other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code.

According to Section 67 of the IT Act, "Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all

[5] India Arrests Its First Ever Cyber Criminal, last visited 17th Aril 2016; http://motherboard.vice.com/blog/india-arrests-its-first-ever-cyber-criminal

relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.[6]

Defamation:

Defamation can be understood as the intentional infringement of another person's right to his good name. It is the wrongful and intentional publication of words or behavior concerning another person, which has the effect of injuring that person's status, good name, or reputation in society. Libel is written defamation and slander is oral defamation. The primary difference is that in libel, damages are presumed, whereas in slander actions, unless the slander falls into a certain category, called slander per se, must prove actual or quantifiable damages.

Cyber stalking:

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyber stalking messages differ from ordinary spam in that a cyber-stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.[7]

The National Center for Victims of Crime (NCVC) suggests that victims of cyber stalking take the following steps:

- For minors, inform parents or a trusted adult
- File a complaint with the cyber stalker's Internet service provider
- Collect evidence, document instances and create a log of attempts to stop the harassment
- Present documentation to local law enforcement and explore legal avenues
- Get a new email address and increase privacy settings on public sites
- Purchase privacy protection software

[6] Cyber Pornography and the IT Act, last visited 18 April 2016 ; https://dict.mizoram.gov.in/uploads/attachments/cyber_crime/cyber-pornography-indian-law.pdf

[7] Cyber stalking, Last visited 18 April 2016; http://searchsecurity.techtarget.com/definition/cyberstalking

- Request removal from online directories
- The NCVC also emphasizes that a victim of cyber stalking should never agree to meet the stalker in person.

Phishing:

The act of acquiring private or sensitive data from personal computers for use in fraudulent activities. Phishing is usually done by sending emails that seem to appear to come from credible sources (however, they are in no way affiliated with the actual source/company), which require users to put in personal data such as a credit card number or social security number. This information is then transmitted to the hacker and utilized to commit acts of fraud. Some of the criminals behind phishing scams have even gone so far as to create websites that appear to be operated by government agencies. Many virus programs and email providers have developed software in attempt to combat the problem.[8]

CONCLUSION

Information Technology has two sides: one the positive side which helps human kind and simplifies their work and the negative side which endangers the identity and other essentials of an individual.

Hackers and cyber criminals have been around almost as long as computers have existed. In recent decades, with advances in technology and the evolution of the internet, cyber-crimes have also evolved in unexpected ways. In today's world, people spend as much, if not most, of their day connected to the internet. Cyber criminals have taken advantage of this by exploiting e-commerce and violating intellectual properties both in the United States and abroad.

News viruses, hacking techniques, and criminals emerge every day. In many cases, the legal system cannot keep up, but it is trying. Initially, the internet was compared to the Wild West, with no rules or laws governing it. Now, cyber law is beginning to catch up, and it is becoming increasingly harder to break the law online. However, the system is not perfect, and it is still much easier to get away with a crime on the internet than it is in real life.

As we have seen by analyzing some of the most relevant laws and cases related to these issues, some aspects of the law are working, and others are not. Technology isn't going anywhere, and people are continuing to spend more time (and money) on the internet. Every time someone is

[8] Phishing, last seen on 19 April 2016; http://www.businessdictionary.com/definition/phishing.html

online, they can be a target of a cyber-criminal. As we have discussed, current cyber law generally does a good job of catching criminals when they are employers working within a victimized company. However, criminals are harder to catch when they are unknown hackers working from anywhere in the world. This is why it is essential to continue working with our foreign allies to strengthen cyber laws not just in our country but in other countries too.

Another area that needs work is laws protecting intellectual property owners against online piracy. Thousands of file sharing sites still exist because they operate in countries where online piracy is legal. We need to focus on these countries and pressurise them to make it illegal for these websites to operate, especially when our citizens have access to them. We can also help by cracking down harder on our own citizens who choose to use these sites to download stolen content.

Cyber-crime and hacking is not going away, if anything it is getting stronger. By studying past incidents, we can learn from them and use that information to prevent future crime. Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cyber-crime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is. Will it be able to remain the same way while becoming tougher on criminals? Only time will tell.

As it is rightly said, "bytes are replacing bullets in the crime world". Cybercrime has been on the rise in India as well as world-wide and to curb its scope and complexity is the need for today's world. Cyber space offers a wide range of opportunities for the cyber criminals to either harm the innocent, or make money by fraudulent means. India's financial status, profile and wealth have risen enormously in the world due to the constructive use of this information technology. With the improvement of technology came an increase in the amount of cyber-crimes. According to a report by the U.S.-based Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center, India ranks fifth in the world for cyber-crime.

Even though the IT Act provides remedies for these cyber-crimes, the investigation is still a challenge. India lacks the resources and what is called "cyber forensics". We know that forensic evidence is very important to prove a case in any normal criminal case. But in India the collection and presentation of electronic evidence to prove a cyber-crime is no less than a challenge for the investigator, prosecution agencies and the judiciary.

To sum up, India needs a good combination of laws and technology, in harmony with the laws of other countries and also keeping in mind reagarding the common security standards. In the era of

e-governance and e-commerce, a lack of common security standards can create havoc for global trade as well as military matters.