International Journal of Law
ISSN: 2455-2194, Impact Factor: RJIF 5.12
www.lawresearchjournal.com
Volume 2; Issue 2; March 2016; Page No. 24-26

Cyber crimes and legal implications

Dr. Jetling Yellosa

Associate Professor, Head and Principal, University College of Law, Telangana University, Dichpally, Nizamabad, Telangana. India.

Abstract
The world has taken dramatic transformation after advent of computers, there is no one in the world who is not touched by information technology. Almost every activity of us is guided and regulated by the computers. There is hardly any facet of our lives that is not touched by the information technology revolution. As the world is depending upon the information technology there is same amount of cyber illegal activities taking place around the world. The Government of India on par with international obligations and statues of comity of nations has enacted a comprehensive enactment called the Information Technology Act of 2000. This Act covers all gamut of information technological matters including curbing of cyber crimes in our country. The Act empowers judiciary to play an important role in curbing the cyber crimes by awarding suitable punishments.
My paper deals with the meaning, details of various types cyber crimes, development of cyber legislation in our country and some important judgments delivered by various courts with matters concerning the cyber crimes and finally I have mentioned suggestions which we have to incorporate in effective curbing of cyber crimes in our country.

Keywords: Transformation, revolution, computer, terrorism, fraud, convention, optical impulses, strategies, jurisdiction, investigation, orthopedist, Pandora box, trafficking, juvenile, gullible

Introduction
Before embarking upon it I would like to deal with meaning of cyber crime: Cyber crime means "unlawful acts wherein the computer is either a tool or a target or both [1]." As name reflects it involves criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, these kinds of crimes are also subject to the Indian Penal code of 1860. The classification of cyber crimes are concerned it can be classified into two kinds, i. the computer as a target, this process the attacker uses a computer to attach another computer, such attacks are commonly known as hacking, virus or worm attacks, disk operating system attacks etc. and the other kind of crime is known as the computer as a weapon, in this process the attacker uses a computer to commit real world crimes which include cyber terrorism, intellectual property law violations, credit card frauds, electronic mail transfer frauds, pornography etc.

Types of Computer Crimes
The computer crimes are classified into different types they are:

1. Trojan horses attack.
2. Back Doors/Trap Doors.
3. The Salami Technique.
4. Logic Bomb.
5. Fraud.
6. Forgery.
7. Hardware/Software Theft.
8. Data Manipulation.
9. Reproduction of a Program.
10. Telemarketing Fraud.
11. Cyber terrorism.

Combating of Cyber Crimes
The world nations have lately awakened to overcome commission of cyber crimes. In international sphere as there is no binding convention or protocol is available to try cyber criminals. But the United Nations made number of attempts to have laws and much persuasion prepared a model law that is endorsed by the General Assembly of the United Nations on 30th of January 1997 and this is only covenants which regulating affairs of cyber crimes.

Cyber Law in India
Until 2000 in our country there is no legislation pertaining to cyber matters. Our country in 2000, has legislated the Information Technology Act of 2000 on par with the model law framed by the United Nations Commission on Trade. The Act is encompasses into thirteen chapters and divided into ninety four sections.
The Information Technology Act 2000 provides a detail meaning of computer and computer network and under section 2(2) it goes on to say that it means an electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, processing, storage, computer software or communication facilities which are connected or relates to the computer in a computer system or computer network.
The Information Technology Act 2000 under chapter XI under section 65 provides the meaning of computer tampering with computer source, it means Who ever knowingly or intentionally conceals, destroys or alters intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer

programmes, computer system or computer network, shall be punishable with imprisonment up to three years, or with fine which extend up to two lakh rupees, or with both. Section 66 of the act prohibits hacking with computer system and Section 67 prohibits publication of obscenity in any form in the computer related activities. The Act also gives wide powers to police officers not below the rank of Deputy Superintendent of Police to any public place and search and arrest without warrant any person found therein committed or committing offences.

Though the proper law is enacted by the parliament which covers every aspect of computer crimes but in our country due to lack of knowledge every minute innumerable computer crimes have been taking place every corner of the country. From recent past in every organization whether private or public all are depending upon the computers and their services, due to which there is alarming growth of crimes.

International Aspects

With the growth in the use of computer networks and the Internet, international aspects of computer crime have received the attention of officials. Computer crime has recently been seen as a global problem. The global nature of computer crime makes domestic solutions inadequate. The identities of perpetrators are often initially unknown, and the space and time dimensions of the intrusions may be unclear. Computer systems can be accessed or destroyed from anywhere and by anyone in the world. This results incomplex jurisdictional issues. These issues require immediate solutions in the international arena. In other words, global issues require global strategies.

Jurisdictional Issues

Jurisdiction is one of the biggest challenges to law enforcement in the information age. "Jurisdiction is the lawful ability of a government to subject a person to that Government's legal processes [2]. Many computer crime incidents involve more than one jurisdiction, which makes it difficult to determine the locus delicti. The crime is committed across the globe it there is issue of conflict of law and which laws have to be applicable trying such offences [3].

Judicial Response to Cyber Crimes in India

The Information Technology Act of 200o clearly stipulates that the cognizance of cases should be taken by the appropriate courts and it is governed by the principles of Criminal Procedure Code. In spite of the act there is not much cases have been filed and tried by the courts in India because of number of factors like ignorance of filing cases, pendency after filing, jurisdictional conflicts, improper investigations on part of law enforcement agencies, lack of knowledge on part of law enforcement and interpretation agencies etc.

Case No. 1: First Case conviction given in the Cyber Crimes

The first case which is filed given of conviction in our country is reported in 2001, in Sony India Private Limited case, brief facts are the Company runs website called sony sambandh targeting nonresident Indians to send different products to friends and relatives in India from foreign countries through online payments. One some in name of Barbara Campa and ordered a television and cordless head phone and the said Barbara had given credit card number requested the products should be delivered to one Arif Azim of Noida. When the payment is to be made the Credit card Company that the card is unauthorized transaction and real owner is denied of transactions. It was revealed that Barbara obtained credit card number of one American and fraudulently availed it. The police filed a case under Section 418,419 and 420 of Indian Penal Code.

The Metropolitan Magistrate court in New Delhi, had felt that as the accused was a young boy of 24twenty four years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year [4].

Case No. 2: First case convicted under Information Technology Act 2000 of India

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.

The Charge 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 twelve witneeses were examined and entire documents were marked.

The Defence counsel argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court based on the expert witness of Naavi and other evidence produced including the witness of the Cyber Cafe owners came to the conclusion that the crime was conclusively proved.

The court has also held that because of the meticulous investigation carried on by the investigating Officer, the origination of the obscene message was traced out and the real culprit has been brought before the court of law

The Additional Chief Metropolitan Magistrate, Egmore, Chennai, 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 [5]."

Case No. 3: Well-known orthopedist in Chennai got life imprisonment

Dr. L Prakash stood convicted of manipulating his patients in various ways, forcing them to commit sex acts on camera and posting the pictures and videos on the Internet. The 50-year-old doctor landed in the police net in December 2001 when a young man who had acted in one of his porn films lodged a complaint with the police.

Apparently the doctor had promised the young man that the movie would be circulated only in select circles abroad and had the shock of his life when he saw himself in a porn video posted on the web.

Subsequent police investigations opened up a pandora box. Prakash and his younger brother, settled in the United States, had piled up close to one lakh shots and video footages, some real and many morphed. They reportedly minted huge money in the porn business, it was stated.

Fast track court judge convicted all the four in Feb 2008, also imposed a fine of Rs 1.27 lakh on Prakash, the main accused in the case, and Rs 2,500 each on his three associates - Saravanan, Vijayan and Asir Gunasingh.

The Judge while awarding life term to Prakash observed that considering the gravity of the offences committed by the main accused, maximum punishment under the Immoral Trafficking Act (life imprisonment) should be given to him and no leniency should be shown.The Judge sentenced Prakash under the Immoral Trafficking Act, IPC, Arms Act and Indecent Representation of Women (Prevention) Act among others [6].

Case No. 4: Juvenile found guilty for sending threatening email

A sixteen year old student from Ahmedabad who threatened to blow up Andheri Railway station in an email message was found guilty by the Juvenile Court in Mumbai.

A private news channel received an email on 18 March 2008 claiming sender as Dawood Ibrahim gang saying a bomb would be planted on an unspecified train to blow it up. The case was registered in Andheri Police station under section 506 of IPC and transferred to cyber crime investigation cell. During Investigation CCIC traced the cyber cafe from which the email account was created and threatening email was sent.

Cafe owner told police about friends which had come that day to surf the net. Police summoned them and found that the system which was used to send email was accessed by only one customer. On 22nd March 08, police arrested the boy a Class XII science student who during interrogation said that he sent the email for fun of having his prank flashed as "breaking news'' on television [7].

Case No. 5: Two Nigerians sentenced seven years RI for online fraud

A local court in Malappuram district in Kerala sentenced two Nigerians to five years rigorous imprisonment on July 20, 2011 in a cyber-crime case. The two had cheated a doctor in the district of Rs 30 lakh about two years ago. Johnson Nwanonyi (32) and Michel Obiorahmuozboa (34), both hailing from Anambra state in Nigeria, were sentenced each under sections 420 (cheating)-5 years, and 468(forgery)-5 years of IPC and section 66(D) (phishing) of Information Technology (Amendment) Act 2008 -2 years and a fine of Rs 1.25 lakh by a Chief Judicial Magistrate V Dileep in Manjeri in Malappuram district. The sentence would run concurrently.

According to the charges filed by the Karipur police, the duo had cheated the doctor Dr. C Thomas, hailing from Valluvambram in Malappuram district after they sent an e-mail asking to pay Rs 30 lakh as processing fee. But a planned move by the police and the doctor succeeded when the Nigerians were lured into Kerala in March 2010. They were then arrested by the Karipur police. The strong evidence based on which the prosecution presented the case became crucial in the first verdict against financial fraud under the Information Technology Act [8].

Conclusions and Suggestions

These above are some of the judgments delivered by the respective courts across in our country. As the incidence of the cyber crimes have increasing by day by day we are seeing filing of more cases across in our country and delivery of innumerable judgments. But in practice if we observe the courts are flooded with number of different kinds of litigations and the adding of cyber crimes to its jurisdiction also causing a strain upon it. The judges and law enforcement officials have not properly well versed with technical spheres of law and they should be trained properly. As the cases have been increasingly manifestly more number of specially trained cyber courts should be established to deal the matters. It is also high time to clearly resolve the jurisdictional matters in the cyber space by suitably amending the Information Technology Act of 2000. The victims of cyber crimes are gullible public and they are not aware of the rules or Act and they should be created of awareness programmes so that they can easily approach the law enforcement agencies for redressal of their grievances.

References

1. www.wikipedia.org
2. Carter and Katz, 2000, Osman N.Sen, Criminal Justice Responses to Emerging Computer Crime Problems, University of North Texas, Page No.59.
3. Supra.
4. http://www.alertindian.com/node/18#gsc.tab=0.
5. http://www.alertindian.com/node/18#gsc.tab=0
6. http://www.alertindian.com/node/18#gsc.tab=0
7. Supra.
8. Supra.