RNI Title Code: TELENG/2017/74418 **ISSN: 2581-6322**

SPWI JOURNAL FOR SOCIAL WELFARE

Volume 1: Issue 1. July – September 2018

Contents

RNI Title Code: TELENG/2017/74418 ISSN: 2581-6322

SPWI JOURNAL FOR SOCIAL WELFARE

Volume 1: Issue 1. July – September 2018

MOBILE CELL PHONES AND CYBER CRIMES IN INDIA

R. Shobha Rani
Research Scholar,
Department of Public Administration & HRM
Kakatiya University, Warangal,
Telangana

Abstract: *In today's world with the advent of Smart Phones there is virtually no difference between Computer and Mobile phones, so whatever Cyber Crime we were aware of related to Computers are also applicable to Mobile Crime. The present paper disclosed the mobile phones and how the cyber crimes are happening in India.*

Key Words: Telecommunication in India, Mobile Phones and human life and its role in cyber crime.

Introduction

Telecommunication was introduced in India long back in the year 1882. There was a mushroom growth of telecommunication after the advent of Internet and Mobile technology in India. It was on 15th August 1995 when the first mobile telephone service started on a non-commercial basis in India. On the same day internet was also introduced in this nation.

After the liberation and privatization in this area India didn't look back, Telecommunication conquered life of citizens of India and in no time India's Telecommunication Network became the second largest in the world. In May 2012 there were 929.37 million mobile users in India. In this dot com era a person is looked with surprise if he is not a mobile user.

Impact of Cell Phones on Human Life

Communication technology has left no aspect of human life untouched. Even our morning alarm clocks are been replaced by the mobile cell phones. Technology is constantly bringing advancement in our mobile cell phones. Mobile cell phones have now become new personal laptops and desktops which are having capacity to store as much data as our laptops and desktops are and in additional they are providing flexibility and portability.

Internet enabled Smart phones, tablets etc… are performing the functions of our computer, but one vital feature is missing and that is Security. Rapid growth in the use of internet enabled mobile cell phones allows us to use manage our banking transaction, official and institutional transactions, rapid communication through email or social networks, and many more. Virtually we can perform the task of a computer on our mobile; this means alike our computer our mobile phone is also vulnerable to the risk of fraud, theft of financial information and identity theft etc.

Cell phones an open door for cyber criminals

Recent reports have suggested that with the advancement of the telecommunication technology there is increase in cyber crime in the nation. The technological advancement provided opportunities to the miscreants in the society, who are using technology for their selfish gains. There are cases where hackers have breached in Nokia's Symbian, Apple's IOS and Google's Android operating system.

Thus to be safe we must be vigilant. But it is really unfortunate that whenever a discussion about cyber crime ignites, a particular class of the people escapes the discussion saying that; they neither use computers nor they use internet for communication and therefore cyber crime is not a threat for them. People try to hide their ignorance about cyber crimes on the ground that cannot become its victim, but they have absolutely no idea that knowingly or unknowingly they can be adversely affected by cyber crime. Every person using an internet, blue tooth or even an infra red enabled cell phone is can easily be fished in the web of cyber criminals.

Definition of Cyber Crime

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 email spoofing and cyber defamation, sending threatening emails etc. a simple yet sturdy definition of cyber crime would be "unlawful acts wherein computer is either a tool or a target or both.

Criminals can operate anonymously over the computer networks, hackers invade privacy, and hackers destroy "Property" in the form of computer files or Records.

- Hackers Injure Other Computer Users by Destroying Information System.
- Computer Pirates Steal Intellectual Property.

Crime Related to the Mobile Technology

- As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not nor necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with criminal element.

  According to Donn Parker, "For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her owen needs."
- The first recorded cyber crime took place in the year 1820. The era of modern computers, however, began with the analytical engine of Charles Babbage. 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 threatening implications.
- The majority of what are termed "cyber crimes" is really violations of long standing criminal law, perpetrated through the use of computers or information networks. The problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of international co-operation to enforce existing laws.
- On the other hand, there are new and serious problems posed by attacks against computer and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate.

  At the same time, it is to be remembered that often the most effective way to counter such as attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information security research and engineering, they could have the unintended consequences of actually undermining information security.

Classification of Cyber Crimes

The Information Technology Act deals with the following cyber crimes along with others

- Tampering with computer source documents
- Hacking
- Publishing of information, which is obscene in electronic form
- Child Pornography
- Accessing protected system
- Breach of confidentiality and privacy

Types of Cyber/Mobile Crime

Cyber crime other than those mentioned under the IT Act

- Cyber Stalking
- Cyber squatting
- Data Diddling
- Cyber Defamation
- Trojan Attack
- Forgery
- Financial crimes
- Internet time theft
- Virus/worm attack
- E-mail spoofing
- E-mail bombing
- Salami attack
- Web jacking

Cyber/Mobile Criminals

Any person who commits an illegal act with a guilty intention or commits a crime is called an offender or a criminal. In this context, any person who commits a Cyber Crime is known as a Cyber Criminal. The Cyber Criminals may be children and adolescents aged between 6 to 18 years. They may be organized hackers, may be professional hackers or crackers, discontented employees, cheaters or even psychic person.

Kids & Teenagers (age group 9 – 16 etc)

- This is really difficult to believe but it is true. Most amateur hackers and cyber crime criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride

to have hacked into a computer system or a website. There is also that little issue of appearing really among friends. These young rebels may also commit cyber crimes without really knowing that they are doing anything wrong.

- According to the BBC, teen hackers have gone from simply trying to make a name for them to actually working their way into a life of crime from the computer angle. According to Kevin Hogan, one of the biggest changes of 2004 was the waning influence of the boy hackers play around with malicious code, 2004 saw a significant rise in criminal use of malicious programs. The financial incentives were driving criminal use of technology.
- Another reason for the increase in number of teenage offenders in cyber crimes are that many of the offenders who are mainly young college students are unaware of its seriousness. Recently the Chennai city police have arrested an engineering college student from Tamil Nadu for sending unsolicited message to a chartered accountant. The boy is now released on bail. So counseling session for college students has to be launched to educate them on the gravity and consequences emanating from such crimes.
- In September, 2005, A Massachusetts teenager pleaded guilty in federal court in Boston for a string of hacking crimes reported to include the February compromise of online information broker Lexis Nexis and socialite Paris Hilton's T-Mobile cellular phone account. The US Court noted that the number of teenage hackers is on the rise and only the lowest 1% of hackers is caught.

Organized hacktivists

Hacktivists are hackers with a particular (mostly political) motive. In other cases this reason can be social activism, religious activism, etc. The attacks on approximately 200 prominent Indian websites by a group of hackers known as Paskistani Cyber Warriors are a good example of political hactivists at work.

Disgruntled employees

One can hardly believe how spiteful displeased employees can become. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire systems down.

Professional hackers (Corporate espionage)

Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation

to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needles if hacking can retrieve those.

Cell phones and the Information Technology act, 2000

As per definition of term Computers, as provided by Sec. 2(i) of the I.T. Act, mobile phones are encompassed in the definition of a Computer. Mobile phones are been used for exchange of information. As per Sec. 2(r) of the I. T. Act, "electronic form", with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device. Thus any information shared on the mobile phone though it may be talks, text or entry of information they are encompassed in the purview of the I. T. Act.

Section 66A of The I.T. Act, provides for punishment for sending offensive messages through communication service, etc. This provision of Law is parallel provision to Sec. 294, 504, 506, 507 & 509 of Indian Penal Code, 1860; only difference is that in these provisions of law the criminal uses his cell phone or computer to express the offensive feeling. The punishment prescribed under this section is imprisonment for a term which may extend to three years and with fine. This section is embedded with an explanation which states that for the purpose of this section, terms electronic mail and electronic mail message means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message. This explanation widens the scope of this section and assures that the criminal cannot escape his liability.

Newly added provision in the I.T. Act in the form of Section 67(A) provides for punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form. This is most important for teenagers. The trends of sharing pornography material on cell phones are on increase. The incident of indecent MMS is not unknown to anyone. This provision of law books those who publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct. This provision of law is analogous to provisions of Sec. 292 and 292-A of the Indian Penal Code, 1860. It provides for a punishment on first conviction for imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees. In the even to second or subsequent conviction for imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

This provision of Law elaborates Section 67 which provides for punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted 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 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 three years and with fine which may extend to five lakh rupees and in the event of 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.

Is Indian law sufficient to handle mobile crime?

- The problem of data theft which has emerged as one of the major cyber crimes worldwide has attracted little attention of law makers in India. Unlike U.K which has The Data protection Act, 1984 there is no specific legislation in India to tackle this problem, though India boasts of its Information technology Act, 2000 to address the ever growing menace of cyber crimes, including data theft. The truth is that our IT Act, 2000 is not well equipped to tackle such crimes. The various provisions of the IT Act, 2000 which deals with the problem to some extent are briefly discussed below.
- **Section 43:-** This section provides protection against destruction and unauthorized access of the computer system by imposing heavy penalty up to one crore. The unauthorized downloading extraction and copying of data are also covered under this section. Clause 'C' of this section impose penalty for unauthorized introduction of computer viruses of contaminants. Clause 'G' provides penalties for assisting the unauthorized access.
- **Section 65:-** This section provides for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer imprisonment of up to 3 years or fine up to 2 lakh rupee. Thus protection has been provided against tampering of computer source documents.
- **Section 66:-** Protection against hacking has been provided under this section. As per this section, hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person an information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This section imposes the penalty of imprisonment of up to three years or fine up to 2 lakh rupee or
- both on the hacker.
- **Section 70:-** This section provides protection of the data stored in the protected system. Protected systems are those computers, computer system or computer

network to which the appropriate government, by issuing gazette information in the official gazette, declared it as protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

- **Section 72:-** This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupee or both.

Can Data theft be covered under IPC?

- ***Section 378 of the Indian Penal Code, 1860 defines 'Theft' as follows:*** Theft – Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.
- **Section 22 of IPC, 1860 defines "movable property" as follows**
- "The words "movable property" is intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth."
- Since section 378 IPC, only refers to "Movable Property" i.e. Corporeal Property, and Data by itself is intangible, it is not covered under the definition "Theft". However, if Data is stored in a medium (CD, Floppy etc.) and such medium is stolen, it would be covered under the definition of 'Theft', since the medium id\s a movable property. But, if Data is transmitted electronically, i.e. in intangible form, it would not specifically constitute theft under the IPC.
- "Data", in its intangible form, can at best be put at par with electricity. The question whether electricity could be stolen, arose before Hon'ble Supreme Court in the case "Avtar Singh vs. State of Punjab (AIR 1965 SC 666). Answering the question, the Supreme Court held that electricity is not a movable property, hence, is not covered under the definition of "Theft" under section 378 IPC.

However, since section 39 of the Electricity Act extended Section 378 IPC to apply to electricity, so it became specifically covered within the meaning of "theft:. It is therefore imperative that a provision like in the Electricity Act be inserted in the IT Act, 2000 to extend the application of section 378 IPC to data theft specifically.

What do we need and why do we need?

It is imperative in today's worlds that an emerging IT super power like India has a comprehensive legislation to protect its booming IT and BPO Industries (worst affected industries) against such crimes. Though the IT Act may appear sufficient in this regard but it is not comprehensive enough to tackle the minute technological intricacies involves in such a crime which leaves loopholes in the law and culprits get away easily. Since this problem is not confirmed to one nation and has international dimensions, India must look forward to be a signatory to any international convention or treaty in this regard. Also if high time that our national police organizations are trained to deal with such crimes

Conclusion

A mobile phone is just like a match stick. A match stick can ignite a lamp and can also ablaze a house. Choice is of the person having it. Alike is with mobile technology you can use it to make you life simpler, or for satisfying you selfish gain by misusing it. As we are careful while using match stick in home, and keep it in safe place out of the reach of children.

A mobile phone also should be used with caution. Your ignorance can bring you in trouble. People must be vigilant and educated towards the game of dirty business played on mobile phones. A certain class of people is exploiting the technology. All the glitters is never gold must be remembered by mobile users. People must be sensitive towards suspicious or malicious information received on their mobile phones. They shall forthwith report against it. This will ensure not only their security but security of others too.

Care also should be taken when we are shopping online; know as much as you can about the site, its policies and procedures. Never share our personal information with stranger on mobile phones. Also no secret information like passwords, PIN, credit card details etc. must be stored on the mobile phone. Precaution is the only means to stay secured in this E-World. In this E-world one must never forget the words of Fransis Bacon that Knowledge is Power, because in the world of computers; more you know about computers, the more you will know that you don't know.

References

- Information Technology act, 2000, Government of India. New Delhi.
- Indian Penal Code, 1860.