Volume 3, Issue 2 ISSN: 2320-5288

International Journal of Engineering Technology & Management Research
Journal homepage: www.ijetmr.org

Cyber Law: Countermeasure of Cyber Crimes

Digbijay Guha
Digbijay Guha
BCA Department
The Heritage Academy
Kolkata, India
Email: digbijay.guha@gmail.com

Shameek Mukhopadhyay
BCA Department
The Heritage Academy
Kolkata, India
Email: shameek.mukhopadhyay@gmail.com

Abstract—From the past few years, crime like traditionally based in the world of physical entity has been increasingly making its way into the world of information. Crime is evolving; since the days when goods were transported by stagecoach, robbery has changed to keep up, even to our modern-day equivalent-credit and debit cards. Internet credit card number theft has become a well-recognized danger. The most common forms of computer crime reported to Inter-GOV include child pornography, fraud, and e-mail abuse. Even more disturbing are new forms of cyber-terrorism made possible by the large amount of the physical machinery now operated by computers. As the countermeasure a system of law and regulations are enacted. In India the act for governing the cyberspace is The Information Technology Act, 2000. In this paper, after attempting to define few computer crimes, legislations of few cyber crimes are discussed from the above mentioned act.

Keywords—Cyber crime; Cyber law; The Information Technology Act; Cyber defamation; Cyber stalking; Phishing; Salami attack; Intellectual property crime; Cyber terrorism

1. INTRODUCTION

Internet is believed to be full of anarchy and a system of law and regulation therein seems contradictory. However, Cyberspace is being governed by a system of law called Cyber law. Cyber law is a generic term which refers to all the legal and regulatory aspects of internet. Publishing a web page is an excellent way for any business to vastly increase its exposure to millions of individuals world-wide. It is that feature of the Internet which is causing much controversy in the legal community.

Cyber law is a constantly evolving process. As the Internet grows, numerous legal issues arise. One of the most important issues concerning cyberspace today is that of Cyber crime.

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Cyber crime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. The field of Cyber crime is just emerging and new forms of criminal

activities in cyberspace are coming to the forefront with the passing of each new day.

Since Cyber crime is a newly specialized field, growing in Cyber laws, a lot of development has to take place in terms of putting into place the relevant legal mechanism for controlling and preventing Cyber crime. **The Information Technology Act 2000** [1] is an Act of the Indian Parliament (No 21 of 2000) notified on October 17, 2000. Some important Amendments were made in **The Information Technology Act 2008** [2].

The Information Technology Act 2000 addressed the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for Cyber crimes

In this article few cyber crimes and their legal countermeasures are discussed.

2. CYBER DEFAMATION

A. Definition

Cyber defamation is publishing of defamatory material against another person with the help of computers or Internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.

B. Legal Issues Involved

Section 66A of The Information Technology Act says that any person who sends, by means of a computer resource or a communication device:-

- any information that is grossly offensive or has menacing character; or
- any content information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
- any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

3. CYBER STALKING

A. Definition

Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, or gathering information that may be used to harass.

A cyberstalker may be an online stranger or a person whom the target knows. A cyberstalker may be anonymous and may solicit involvement of other people online who do not even know the target.

Technology ethics professor Lambèr Royakkers writes that:

"Stalking is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly

traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)." [3]

B. Legal Issues Involved

In India, The Information Technology Act 2008 (amended) does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in The Information Technology Act 2008. Hence the most used provision for regulating cyber stalking in India is section 72 of the Information Technology Act (Amended), 2008 which runs as follows;

Section 72: Breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, r e gi st er, c orrespon denc e, information, document or other material without the consent of the person concerned discloses such electronic record, book, r e gi st er, c orrespon denc e, 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.

And also section 72A of The Information Technology Act, 2000(amended in 2008), which runs as follows:

Section 72A:Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008): Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

4. CHILD PORNOGRAPHY

A. Definition

Child pornography refers to images or films (also known as **child abuse images**) and, in some cases, writings depicting sexually explicit activities involving a child. Abuse of the child occurs during the sexual acts which are recorded in the production of child pornography.

Legal definitions of child pornography generally include sexual images involving pre-pubescent and pubescent or post-pubescent minors and computer-generated images that appear to involve them.

B. Legal Issues Involved

Child pornography in India is illegal. In February 2009, the Parliament of India passed the Information Technology Bill," banning the creation and transmission of child pornography. The bill enables India's law enforcement agencies to take strict action against those seeking child pornography. For example, browsing for child pornography on the Internet can lead to a 5 year term of imprisonment and a ₹ 40 lakh fine [4].

In India, distributing pornography is illegal. However, enforcement is extremely lax and pornographic materials are easily available in public places. Softcore and hardcore pornography movies/photos are easily accessible through magazines, films, or Internet. The law states that possessing and watching pornographic materials is

legal, but production and distribution are prohibited.

Pornographic films in India are referred to as Blue Films and are available virtually anywhere; especially in areas where pirated material is already being sold. Despite the illegality, stores selling X-rated material are abundant in major cities and advertise openly; laws are rarely enforced in this case. However, in 2010, Bombay High Court ruled that watching pornography is legal.

Section 67 of **The Information Technology Act** deals with **"publishing obscene information in electronic form"**. This law has been interpreted to criminalize the posting of pornographic content online. However, accessing "obscene" content privately is not illegal. The Information Technology Act was amended by the Parliament on 2008, and **Section 67B** was inserted which **criminalizes browsing, downloading, creating, and publishing child pornography**. Child anime porn is also explicitly criminalized.

5. PHISHING

A. Definition

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Voice phishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.

SMS phishing uses cell phone text messages to deliver the *bait* to induce people to divulge their personal information.

B. Legal Issues Involved

66 A Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device:-

a) any **information** that is grossly offensive or has menacing character; or

b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

c) **any electronic mail or electronic mail message for the purpose** of **causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)**

shall be punishable with imprisonment for a term which may extend to three years and with fine.

66 C Punishment for identity theft.

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and

shall also be liable to fine which may extend to one lakh rupees.

6. SALAMI ATTACK

A. Definition

Salami attacks take place when small, almost immaterial, amounts of assets are systematically acquired from a large number of sources. In such miniscule denominations, they frequently exist just below the threshold of perception (and detection, for that matter). The result is an ongoing accumulation of assets in such a manner that the victims, whose assets are vanishing, fail to even notice.

B. Legal Issues Involved

Section 66 Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section, -

1. the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

2. the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Section 43 (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network.

7. INTELLECTUAL PROPERTY CRIMES

A. Definition

Intellectual Property crime is more generally known as counterfeiting and piracy. Counterfeiting is, willful trade mark infringement, while piracy involves, willful copyright infringement. These are very similar and often overlapping crimes. IP crime is not a new phenomenon but due to globalization and advances in technology counterfeiting and piracy has become big business.

B. Legal Issues Involved

India continues to remain on the priority watch list of the US Trade Representative, meaning that India is perceived as not providing adequate intellectual property rights protection or enforcement of laws protecting IPR. However the admitted experience of IP crime in India is lower than in Asia-Pacific region and globally and is contrary to general perception of the relative incidence of IP crime in India. While India does not have a separate legislation to address counterfeiting as in the US, it offers statutory remedies, both civil and criminal which are embodied in the new Trademarks Act of 1999, The Copyright Act, 1957, The Patents Act 1970, The Designs Act 2000, The Geographical Indications of Goods (Registration and Protection) Act 1999, Custom & Border measures are provided in The Customs Act, 1962 which one can access through various IP statutes. India has made important changes to its IP laws and more are in the pipeline, including changes in IP and Customs laws to implement border control measures as required by the TRIPs Agreement [5]. India has signed Customs Mutual Assistance Agreement with most of its major trade partners including EU & USA. These treaties establish formal guidelines and allow officials to share intelligence and investigative data relating to IP violations. In addition, in the last five years the Indian courts have taken a more pragmatic approach to counterfeiting. Lobbying by various brand owners ' associations, and more education programmes have resulted in increased awareness and a greater understanding of IP issues among law enforcement authorities.

While crimes such as drug dealing and trafficking are viewed with great concern, the general perception in India of IP crime is that it is a "victimless crime". Consumers in the India still appear to be relatively unconcerned because of a divergence of public perception and the lack of understanding about the effects of IP crime. Recently there have been stronger signals with lengthier sentencing and higher penalties for those convicted of counterfeiting and piracy. However, mixed messages are still conveyed and lower penalties are more common than those imposed for more high profile criminal activities.

8. CYBER TERRORISM *A. Definition*

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

B. Legal Issues Involved

66F. Punishment for cyber terrorism, The Information technology Act, 2000 states that (1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a com put e r r eso ur c e wi t ho ut aut ho ri z at i on or ex ce edi n g authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

9. CONCLUSION

Actually above discussed issues contain some underlying problems. Since Cyber crime is ―international‖ or ―transnational‖ i.e. there are ―no cyber borders between countries‖, International cyber crimes often challenge the effectiveness of domestic and international law and law enforcement. Non-existence of global standards of legislation and law enforcement both on a regional and on an international scale help cyber criminals continuing with the criminal activities in cyberspace.

To overcome these problems international cooperation for fighting cyber crime is highly required.

There should be global standard for technical issues.

Global Cyber Law should be implemented.

For maintaining the global Cyber Law proper Law Enforcement should be formed. One suggestion for that Law Enforcement is World Cyber Cop. Special Task Force should be implemented with the help of the representatives from all the countries' police force. This Special Task Force should not be bounded by any territorial jurisdiction.

Most importantly Global Cyber Courts should be established. There should be a World Tribunal which should control all the Country Tribunals which in turn should have many Regional Tribunals.

REFERENCES:

[1] The Information Technology Act 2000, Bare Act

[2] The Information Technology Act 2008, Bare Act

[3] htt p:/ /en . wi ki pedia . org/ wi ki / Cyberstalking (last access date on 15-09-2015)

[4] htt p:/ /en . wi ki pedia . org/ wi ki / Child_pornography_laws_in_India (last access date on 16-09-2015)

[5] http://www.mondaq.com/india/ x / 3 2 1 1 1 2 / T r a d e m a r k / IP+CRIME+Rising+Threats+To+I ntellectual+Property+Rights (last access date on 21-09-2015)