In-depth Analysis of an Indian I.T. Act Related to Unauthorized Access

Aaruni Goel
IIMT Engineering College
Meerut, India

Ashok Vasishtha, PhD.
IIMT Engineering College
Meerut, India

Manish Gupta
Moradabad Institute of Technology
Moradabad, India

ABSTRACT

Cyber Laws are the laws prevailing in the cyber space. Cyber space has a vast definition which encompasses the term like computers, computer networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines, satellites, Microwaves etc. These Laws covers firstly that they must be standardized by government. Secondly should be in force under some specific region and finally must be obeyed by all persons under such specified region. Any violation of these rules could give the right to government to take action such as imprisonment, or fine or an order to pay compensation as per specified through proper Legal jurisdiction. In India, in general the major concerned on Cyber Laws is on Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, Data Protection and Privacy. It should be noted all that cyber crimes are unlawful in which computer or any resource attached to it, is tampered. Here devices of both attacker and victim are important evidences also. At last the term crime and the punishment to criminal in such offence can vary from country to country. It is so because the Constitution of any country is a law of land where land is the territory of that country.

Keywords: Computer Networks, MAC Spoofing, IP Spoofing, Firewalls, Intrusion Detection and Prevention Systems (IDPS), Key Loggers, Hacking, Trojans, Constitution of India.

1. Introduction

In India a Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. It handles those crimes, which accomplishes with the help of computer, computer system, computer network, internet, storage devices or communication device. The I.T. Act in India has no very strict definition. But all it includes cyber contraventions and cyber offences. For e.g. cyber contravention is in general describes to any unauthorized access may or may not come under law and is of degree of penetration to lesser (may be not to harm or for educational research purpose) extent while in case of cyber crimes they are the exploits for gaining unauthorized access intentionally to harm. It should be noted that in Indian context the punishment under for cyber crimes is also given on the basis of Indian Penal Code (IPC) which is also a constitutional legal hand book to prosecute criminals engaged in other social crimes[1].

Are Cyber Laws Self Sufficient?

There are many scenarios in which it has been thought worldwide to draft and implement act . Many of the laws formulated so far are acting perfectly but still there are many other problems that the world is facing in drafting such laws like[2][3][7]:

1. Cyberspace is not yet properly definable so still it is not very practical to manage it by through conventional laws or Constitution by the Government of many countries.

2. Before drafting Cyber laws pertaining to different countries, all responsible countries should consider that what should be effects and implications of such laws across geographical and jurisdiction boundaries. Further enormous amount of data traffic flow over the Internet is based on just simple click where by many times a criminal can clear the tracks to being captured

3. In making cyber laws it should also be considered that distance and anonymity does not matter. Any person throughout the world can communicate with any person irrespective of distance and secrecy.

4 The Financial crimes are more prevalent in internet now a days. So cyber laws specially in such issues look after that the transfer of such money is under any Financial law or not.

5. A Cyber Law under software or movie or copyrighted materials piracy issues should be also evaluated before formulating of cyber laws.

In this paper we will like to project out some access related Cyber laws and punishments that are prevailing in Indian Territories under I.T. Act. It also has been tried out that the understanding of unauthorized to be best explained with proper Analogies and Examples .

2. Access related crimes in India

According to section 2(1)(a) of the IT Act "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network [1];

Here access simply describes right to use the computer or any other resource attached to that computer whether in terms of executing any command or in terms of any communication through computer, computer system or computer network which is/are logical, arithmetical, or memory function. Additionally the term access not only limited to the aforesaid explanation but also applicable to any physical touch to computer or any resource attached to it.

It should be noted that as per law grammatical variations means that term access can also be replaced by its noun, verb, adjective or any grammatical form. Further cognate expressions are synonyms or the words related to name ‘access’ e.g. entrance, sign in, start etc. All the

grammatical variations and cognate expressions are used according to the situation or circumstances observed [1].

2.1 Unauthorized Access

According to section 43(a) of the IT Act

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) accesses or secures access to such computer, computer system or computer network; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected [1].

Here the term secure access means that any person who is sure that that he can access the system and whenever he wants from anywhere without permission.

Analogies:

1. To access computer system remotely with the help of Trojans.
2. Through application of Social Engineering on friends, relatives etc.
3. With the help of hacking through any software or otherwise e.g. by using telnet or ftp commands.
4. By e-mail spoofing or MAC spoofing or IP spoofing.
5. By knowing passwords with the help of Key loggers or Shoulder Surfing

Now we will like to define term 'permission'. It can be Full, Partial or Implied.

Analogy

The best example to understand this term is Intranet. In our college each faculty has separate Log-in ID and password. There is also a Director Log-in which reserves the full right to verify records of marks, attendances etc. of students that are uploaded by concerned faculty of concerned subject(s) of whole college. He further can add, delete or modify any uploaded data of faculty if found with error or in case of any discrepancy. Now

1. Director Log-in has Full permission to access anybody's account.
2. Management of College authorized Director Log-in to confer full right to access any faculty record. This comes into partial and Implied categories of permission. In regard of Implied it means that Director can access any record of faculty but it is also a Partial permission since he has to look out only academic activities of faculties for e.g. he is not authorized to view the salary status or any financial transaction of faculty which is under the control of accounts department.
3. There is only one scenario which comes under unauthorized access. Suppose Director is on leave and he gives his Log-in Id and password to his assistant. But due to some malaise intention he modified the data of a particular faculty.

The only way to find out that what had happened that day is the Log recovery through IDPS [10].

The penalty provided for this section is compensation up to Rs 1 Crore.

2.2 Accessing Protected System

According to section 70 of the IT Act

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-Section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this Section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine as per Executive order dated 12-9-2002, issued by Ministry of Communications and Information Technology [1].

In this section according to the Constitution of India a new terminology comes out i.e. appropriate government. As per the Constitution of India under Schedule VII there are three lists, mentioned to work out for Citizens welfare – (i) List under Central Government e.g. Foreign affairs etc. , (ii) List under State Government e.g. Police Department etc. and (iii) Concurrent List under both Central and State Government e.g. Forestry etc.. Therefore, appropriate Government means that which Government has the execution power according to the list mentioned above.

The Official Gazette is a document where all the notifications etc. passed by the Central and State Government are reported. A notification becomes effective on the date of its publication in the Gazette and this order may spell out the authorized persons by name or by designation for their new action plan [5].

One more thing which comes out in picture is 'Attempt' to secure access. Attempt means to make an effort to accomplish something. This effort is successful or not it is immaterial provided that there is no any type of legal permission given as stated above.

The punishment provided for this section is rigorous or simple imprisonment of up to 10 years and fine[2][4].

2.3 Hacking

According to section 66 of the IT Act

(1)Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2)Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two Lakhs rupees, or with both[1].

Here the term Loss implies any type of harm can be provisional or permanent. For e.g. someone deleted the Director's confidential data fro his pen drive but by using any data recovery software Director regenerate his data. This is Provisional or temporary loss but if some body hammered or stolen the pen drive then the data loss is permanent.

Loss can be guessed as that individual will suffer either in present or likely to be in future. This loss can be in the

form of financial assets, reputation. For e.g. somebody launches the DDoS attack on any famous spare parts manufacturing company ABC's server. Due to this attack employees and management are neither able to read messages nor any customer or dealer can book the orders. Frustrated customers leave the website and book their orders in other company with same profile. In this case company ABC will suffer both financial and reputation loss.

Another term Wrongful loss in this section is the loss by any unlawful means. For e.g. somebody gains unauthorized access to Network Administrator's system and change the settings of Firewalls and many other settings which opened the path for hackers.

The term Damage is defined as any injury or weakening caused by an unlawful act with malaise intention (see term Intent in this section) and not accidentally. For e.g. Director orders his assistant to copy some large files in his Pen drive and then he goes for lunch. After copying the files the assistant accidentally broken the pen drive's computer interface during unplugging pen drive. This scenario is not considered as damage according to the law. But if he does this with malicious intention then it will be considered as 'damage' and will come under legal jurisdiction.

The term Cause can be any type of basis to make happen something and can effect directly or indirectly. For e.g. somebody formats Director's System and there by all the data is deleted. This is direct cause of data deletion.

A faculty sent a mail to Director which contains virus. This happens accidentally. But due to this the virus corrupts and deletes the computer system of Director. This is Indirect cause of data deletion.

The term 'Knowingly' describes to do something with strong malicious determination.

The term 'Likely to cause' implies probability of cause and is based of circumstances observed during Cyber Crime Investigation.

The term 'Public' means People. If somebody for e.g. hacked the cellular service provider website and made the server down, this means public is affected. Other example In Cyber café owner runs a installs a program which can record all the data typed by users. In this case this is a crime since it affects the privacy of public.

The term 'Destroy' means to make the information stored in computer futile while the term deletes means to erase information permanently or provisionally. Like wise term Alteration can be permanent or temporary. The term 'Value' means financial worth of data on the other hand the term Utility means importance of data.

Lastly the hacking means to find weaknesses in a computer or computer network and attempt to break the computer or computer networks for unauthorized access or otherwise. This term has very wide coverage in Indian Cyber laws.

The punishment provided for hacking is imprisonment up to 3 years and / or fine up to Rs two Lakhs.

2.4 Assisting Unauthorized Access

According to section 43(g) of the IT Act

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected [1].

The essential element of this section is that assistance is provided for obtaining access to a computer in contravention of the IT Act and its allied laws.

A person who obtains access to a computer in contravention of the IT Act would be liable under the relevant sections (e.g. 43(a) or 66 or 70 etc).

What this section specifically covers is providing assistance to such a person so that such assistance facilitates the unlawful access.

Under this section of Indian Cyber Laws this comes under the Breach of privilege. Here the two terms Assistance i.e. the act of 'helping' and 'facilitate' i.e. the approach to provide any aid to complete the task, are also mentioned.

It is like that to obtain passwords or any confidential details related to protected systems from close friends or relatives etc. in order to oblige him/her some financial or moral obligation i.e. to obtain confidential information by using such passwords or to manipulate Firewalls or intrusion Detection System settings and so on.

It has been seen that all these acts are unlawful access provided by the disgruntled employee or nay traitor inside the organization.

The penalty provided for this section is compensation up to Rs one crore.

Some important case studies which have been registered in courts of law under Indian Cyber Laws are detailed down. Further they also describe the concept of terms 'hacking' and 'unauthorized access' [11].

1. A displeased employee of a bank putted down a strong magnet near the banks' main server. After sometimes the bank lost the important information related to customers account.
2. Two persons were allegedly arrested in 2002. They used password cracking software to crack the FTP password for the Mumbai police website and then change the homepage of this website with pornographic content.
3. The Delhi Municipal Corporation (DMC) is on be half of electricity department is used to collect money provided receipts and performed accounting of Electricity bills through Computer Systems. When this process is transferred to private party then one of them who was Computer Expert dispensed large amount of funds by manipulating data files to show less receipt and bank remittance.
4. A young lady reporter was in trap when during online surfing related to her articles, she was victimized by somebody. Some one installed Trojan in her computer. This lady computer was located in one corner of her bedroom. Every time Trojan activated when she starts her internet connection. This Trojan further starts her web cam

and microphone without her knowledge The connection further works when she use to disconnect her internet connection. Later she came to know that many of her pictures and videos were transferred to pornographic websites.

5. India witnessed its first cybercrime conviction recently in 2002. This all started when Sony India Private Ltd. ran website called www.sony-sambandh.com. The aim of this website was to sending Sony products to their friends and relatives in India through online payment. In May 2002, someone logged onto the website under the identity of Barbara Campa and placed a order of Sony Colour Television set and a cordless head phone and made online payment through Credit Card for Arif Azim, Noida The payment was cleared by the credit card agency and the transaction processed. After following the relevant procedures, the Sony company delivered the items to Arif Azim. But after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The Sony Company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the colour television and the cordless head phone and Arif was arrested [8].

3. Conclusion

One of the greatest hurdle in the field of Cyber Crime is the absence of comprehensive law throughout the World. Further the immense growth types of attacks and cyber crimes make the situation more complicated. Though a beginning has been made by the enactment of I.T. Act and amendments made to it provide more powers but still problems associated with cyber crimes continue. In this scenario there is a need of understanding Cyber attacks and their Technical specifications by Police/Intelligence Departments and Judges. A recent positive response has been shown by Kerela High Court which accepted the P.I.L. (Public Interest Litigation through an email [2][8].

In India itself those sections, where the imprisonment term is upto three years have been made bailable. Thus offences committed under sections 65, 66, 66A, 66B, 66C, 66D, 66E, 67 (first conviction), 67C, 68, 69B, 70B, 71,72,72A, 73 & 74 are bailable. Non-bailable offences are sections 66F, 67(second conviction), 67A, 67B, 69,69A, and 70. Hacking is an offence under the provisions of I.T. Act and comes under wider clauses. For e.g. it can be referenced as part of section 65 'tampering of computer source code', section 66 'computer related offences', section 66B 'dishonestly receiving stolen computer resource etc.', section 66C 'identity theft', section 66D 'cheating by personating by using computer resource', & section 66F 'cyber terrorism' [1][4].

It should also be noticed that hacking and ethical hacking are same as per the section 66 of this Act. Again both 'hacking' and 'ethical hacking' could be treated as computer related offences as expressed under section 66 of the Act. It is also possible that based upon the set of circumstances, an incident of ethical hacking may result from unauthorized access to computer, computer network or computer resource and thus can be classified as cyber contravention also as mentioned under section 43 of the Act. We will also like to mention here that under section 66A telemarketers, sending SMSs, Emails etc. are also come under legal jurisdiction of Cyber laws in India since any person who sends, by means of a computer resource or a communication device any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience shall be punishable with imprisonment for a term which may extend to three years and with fine.

At last the education and training of Security experts, IT professionals, curious students should be centered about secured technical knowledge and skills. It is up to his or her duty that what he or she is going to decipher. So it is for all those who thinks that for what purpose they are entitled to access information i.e. lawful or unlawful.

4. References

[1] Indian I.T. Act, 2008(Amendment).

[2] Duggal, Pavan, Cyber Law: The Indian Perspective, 2009. Saasksar Publications.

[3] www.asianlaws.org.

[4] Gaur, K.D A text book of the Indian Penal Code, Universal Law Publishing Company Pvt. Limited, Apr-2004.

[5] Ashok Felix, The Constitution of India, 2011.

[6] Godbole, "Information Systems Security", Dec-2008, Willey

[7] Sood, "Cyber Laws Simplified",2011, Mc Graw Hill

[8] Singh,Talwant, Cyber Law & Information Technology, District & Sessions Judge, Delhi.

[9] Gaur, K.D. , Criminal Law and Criminology, Deep and Deep Publications, 2003

[10] www.wikipedia.org

[11] www.cybercellmumbai.com