© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Cyber Security : Protection of Human Rights

Navjot Jyoti
Assistant Professor, Department of Computer Science & Engineering, Northwest Group of Institutions, Dhudike, Moga, Punjab, India

ABSTRACT

Presently, it is basic to share data publically on the web. There are numerous social sites which are utilizing person's information to show publically. Although each site clarifies their privacy policies however everybody doesn't know from these points of interest. Thus, there are numerous breaks to person's data. At the point when data is access by unapproved people utilizing Computer as well as Internet then it is a crime known as a cyber crime. It is our right to keep the information private and if someone is rupturing the security of other without approval then it resembles violations of human rights. This article gives information about cyber crime, privacy, right to privacy, and protection of this private data of individuals by National Cyber Security Policy.

Keywords: Cyber Security, Human Rights, National Cyber Security Policy, Cyber Phishing

I. INTRODUCTION

Computer crime, or **cybercrime**, is any crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target.[2] Cyber crime is any criminal activity in which a computer or network is the source, target or tool or place of crime. According to The Cambridge English Dictionary cyber crimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Crimes which involve use of information or usage of electronic means in furtherance of crime are covered under the ambit of cyber crime. Cyber space crimes may be committed against persons, property, government and society at large but still Cyber Crime is neither defined in the IT Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India [4].

The common types of cyber crimes are:-

1. **Hacking** – An unauthorized user who attempts to or gains access to an information system is known as hacker. Hacking is a cyber crime even if there is no visible damage to the system, because it is an invasion in to the privacy of data.

2. **Cyber Stalking** – Cyber stalking involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.

3. **Spamming** – Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates negative impact on consumer attitudes towards Internet Service Provider.

4. Cyber Phishing – It is a criminally fraudulent process in which cyber criminal acquires sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

5. Software Piracy – It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies. There are numerous cases of software piracy. In fact according to one report New Delhi's Nehru market is the Asia's largest market where one can easily find pirated software.

6. Corporate Espionage – It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.

7. Money Laundering – Money laundering basically means the moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. This is possible prior to computer and internet technology and now times electronic transfers have made it easier and more successful.

8. Embezzlement - Internet facilities are misused to commit this crime. It is the unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offender's care, custody or control.

9. Password Sniffers – These are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.

10. Spoofing – Spoofing is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted.

11. Credit Card Fraud – In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases. In present world this cyber crime is emerged as a major threat as numerous cases had been filed in almost every major developed and developing country.

12. Web Jacking – The term refers to forceful taking of control of a web site by cracking the password.

13. Cyber terrorism – The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country [3].

Cyber Crime as Human Rights Violations

At the point when any one carrying out the crimes utilizing Internet and Computer is known as a cyber-crime. In Indian constitution under article 21, right to privacy is the part of basic rights. In the event that anybody is carrying out the crime utilizing some electronic media then it is specifically violations of human rights. There are such a large number of things to keep protected from others access to characterize the limits of somebody's data. Subsequently unapproved access of this data is at last violations of human rights which ought to be ensured as other crucial rights are secured.

What is Privacy?

Security with the end goal of this paper could especially be characterized as the desire that private individual data uncovered by any person to Government or non-Government substance ought not be revealed to outsiders without consent of the individual and sufficient safeguards need to be adopted while processing and storing such information. Basically, exposure of information which can be utilized to distinguish a physical individual

without following the due strategy could be understood as break of security [6].

Right to privacy

Right to privacy is an important natural need of every human being as it creates boundaries around an individual where the other person's entry is restricted. The right to privacy prohibits interference or intrusion in others private life. The apex court of India has clearly affirmed in its judicial pronouncements that right to privacy is very much a part of the fundamental right guaranteed under article 21 of the Indian constitution [4].

For a better understanding of the concept of privacy in relation to this study, I refer to the classification of Clarcke[6] in the following dimensions:

- Privacy of the person: sometimes referred to as 'bodily privacy'. This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization;
- Privacy of personal behaviour. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy';
- Privacy of personal communications. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'; and
- Privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.

Is there a need for privacy protection?

India does not currently have a general data protection statute. Nevertheless, the judiciary has derived a "right of privacy" from the rights available under Articles 19(1)(a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution of India. However, all cases that deal with the right to privacy have been decided in the context of Government actions that resulted in private citizens being denied their right to personal privacy. No privacy judgment has granted private citizens a right of action against the breach of privacy by another private citizen. To that extent, the data protection and personal privacy jurisprudence in the country is not yet fully developed.

India is not a particularly private nation. Personal information is often shared freely and without thinking twice. Public life is organized without much thought to safeguarding personal data. In fact, the public dissemination of personal information has over time, become a way of demonstrating the transparent functioning of the government. While many agencies of the government collect personal data, this information is stored in silos with each agency of the government maintaining information using different fields and formats. Government databases do not talk to each other and given how differently they are organized, the information collected by different departments cannot be aggregated or unified.

Data privacy and the need to protect personal information is almost never a concern when data is stored in a decentralized manner. Data that is maintained in silos is largely useless outside that silo and consequently has a low likelihood of causing any damage. However, all this is likely to change with the implementation of the UID Project. One of the inevitable consequences of the UID Project will be that the UID Number will unify multiple databases. As more and more agencies of the government sign on to the UID Project, the UID Number will become

the common thread that links all those databases together. Over time, private enterprise could also adopt the UID Number as an identifier for the purposes of the delivery of their services or even for enrollment as a customer. Once this happens, the separation of data that currently exists between multiple databases will vanish.

Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data before the vast government storehouses of private data are linked up and the threat of data security breach becomes real.

Similarly, the private sector entities such as banks, telecom companies, hospitals etc are collecting vast amount of private or personal information about individuals. There is tremendous scope for both commercial exploitation of this information without the consent/ knowledge of the individual consent and also for embarrassing an individual whose personal particulars can be made public by any of these private entities. The IT Act does provide some safeguards against disclosure of data / information stored electronically, but there is no legislation for protecting the privacy of individuals for all information that may be available with private entities.

In view of the above, privacy of individual is to be protected both with reference to the actions of Government as well as private sector entities [6].

Is there is constitutional right to Privacy?

In certain countries, such as South Africa and Argentina, the right to privacy is incorporated into the constitution. In India, the right of privacy has been derived through judicial decisions, from the rights available under Articles 19(1) (a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution. There was no specific discussion on the concept of privacy in the Constituent Assembly Debates. However, over time, the Supreme Court has held that even though the right to privacy is not expressly enumerated as a fundamental right, it could certainly be inferred from the fundamental rights guaranteed under the Constitution.

Article 19(1)(a) states that -

- All citizens shall have the right to freedom of speech and expression.
- The Supreme Court has, through a series of decisions held that, even though the right to privacy was not enumerated as a fundamental right, it could certainly be inferred from the fundamental rights of the Constitution. However, these fundamental rights are not without restrictions. Just as Article 19(1) (a) bestows on each citizen the fundamental right of freedom of speech and expression, Article 19(2) imposes restrictions on this right. It states that:
- Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in 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.
- The necessary implication of this is that the Government can deprive a citizen of his constitutional right of freedom of speech and expression for any of the reasons set out in Article 19(2). By natural extension of this principle, the Supreme Court, in Gobind v. State of Madhya Pradesh, held that a violation of personal privacy is possible with the sanction of law.
- However this position was clarified and extended in People's Union of Civil Liberties v. the Union of India where the right of government authorities to intercept, in the interests of national sovereignty, messages transmitted or received by any telegraph, was challenged in the context of wire tapping. The Supreme Court held that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave

circumstances such as in the case of a public emergency. This case was significant in that while the court upheld the restrictions on the fundamental freedoms that have been guaranteed under the constitution, it insisted that the government must use restraint in exercising these powers.

- All available cases on this point have been decided in the context of government actions that resulted in the deprivation of personal privacy of individuals. There has been no case decided in the context of the infringement of personal privacy by private citizens. It is therefore unclear as to how these precedents will apply in such cases [6][9].

National Cyber Security Policy 2013

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India. It aims at protecting the public and private infrastructure from cyber attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

The National Cyber Security Policy of India 2013 is suffering from various shortcomings and limitations as per various studies and researches. Despite the declaration of the policy, India is still not cyber prepared. The policy has also not been implemented till the month of November 2014 (till 21 November 2014). The cyber security challenges in India would increase further and immediate action is required in this regard. The proposed initiatives like National Cyber Coordination Centre and National Critical Information Infrastructure Protection Centre (NCIIPC) of India could prove useful in strengthening Indian cyber security and critical infrastructure protection in India [8].

Objective[8]

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
- To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.
- To create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training.
- To provide fiscal benefit to businesses for adoption of standard security practices and processes.
- To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of

law enforcement capabilities through appropriate legislative intervention.

Shortcomings[9]

The National Cyber Security Policy 2013 has failed to address numerous issues as per various research and analysis. Some of these issues are:

(1) The declared cyber security policy has proved to be a paper work alone with no actual implementation till date.

(2) The cyber security trends and developments in India 2013 (Pdf) provided by Perry4Law's Techno Legal Base (PTLB) has listed the shortcomings of Indian cyber security policy in general and Indian cyber security initiatives in particular.

(3) Indian cyber security policy has failed to protect civil liberties of Indians including privacy rights.

(4) Civil liberties protection in cyberspace has been blatantly ignored by Indian government and e-surveillance projects have been kept intact by the Narendra Modi government.

(5) The offensive and defensive cyber security capabilities of India are still missing.

(6) India is considered to be a sitting duck in cyberspace and cyber security field and the proposed cyber security policy has failed to change this position.

(7) Over regulation, ICT Supply Chain risks, absence of adequate testing facilities of electronic equipments, lack of stress upon international cooperation, etc are some other concerns that have been raised by the Data Security Council of India.

(8) The NCSP's poor drafting and meaningless provisions do not advance the field.

In short, India is not at all cyber prepared despite the contrary claims and declared achievements and the cyber security policy is just another policy document with no actual implementation and impact.The cyber security challenges in India would increase further and immediate action is required in this regard.

Who owns the information I put on these sites?

Since Facebook and other social communication sites are generally new and always showing signs of change their protection approaches it isn't totally certain who claims the data you share. In its Statement of Rights, Facebook states, "You possess the greater part of the content and data you post on Facebook, and you can control how it is shared through your protection and application settings." in the meantime, it proclaims that clients allow the organization "permit to utilize any IP content that you post on or regarding Facebook." at the end, you in fact claim the content, however Facebook can do whatever it needs with it.

Facebook states it doesn't have your data after the cancellation of your account, yet that any individual data or pictures you've shared to different clients remains the property of Facebook. This absence of clearness makes everything the more critical that what data you truly need to share. The main issue is: when utilizing any social networking site, you should consistently read their security approach to see how your data is dealt with. More often, it is up to you to opt out of having your information shared[7].

Penalties and Offences, Section under IT Act, 2000 Offence Penalty

Sec.43 Damage to computer, computer system, etc. Compensation not exceeding one crore rupees to the person so affected

Sec.43A Body corporate failure to protect data Compensation not exceeding five crore rupees to the person so affected

Sec.44(a) Failure to furnish document, return or report to the Penalty not exceeding one lakh and fifty thousand rupees for each such failure Controller or the Certifying Authority

Sec.44(b) Failure to file any return or furnish any information, books or other documents within the time specified Penalty not exceeding five thousand rupees for every day during which such failure continues

Sec.44(c) Failure to maintain books of account or records Penalty not exceeding ten thousand rupees for every day during which the failure continues

Sec.45 Where no penalty has been separately provided Compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees

Sec.65 Tampering with Computer source documents Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both

Sec.66 Hacking with Computer systems, Data alteration etc. Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both

Sec.66A Sending offensive messages through communication service etc. Imprisonment for a term which may extend to three years and with fine

Sec.66B Retains any stolen computer resource or communication device Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both

Sec.66C Fraudulent use of electronic signature Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh

Sec.66D Cheats by personating by using computer resource Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees

Sec.66E Publishing obscene images Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Sec.66F Cyber terrorism Imprisonment which may extend to imprisonment for life.

Sec.67 Publishes or transmits unwanted material Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees & in the event of a 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.

Sec.67A Publishes or transmits sexually explicit Imprisonment for a term which may extend to five years and with fine material which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

Sec.67B Abusing children online Imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

Sec.67C Preservation of information by intermediary Imprisonment for a term which may extend to three years and shall also be liable to fine

Sec.70 Un-authorized access to protected system Imprisonment for a term which may extend to ten years and shall also be liable to fine

Sec.71 Misrepresentation to the Controller or the Certifying Authority for obtaining license or Electronic Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Sec.72 Breach of Confidentiality and Privacy Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Sec.72A Disclosure of information in breach of contract Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both

Sec.73 Publishing false digital signature certificates Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

II. REFERENCES

[1]. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[2]. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5

[3]. http://cybercellmumbai.gov.i accessed on 1 Dec 2013
[4]. http://www.lawctopus.com/academike/cyber-crimes-other-liabilities/
[5]. Paper by Roger Clarcke, National University of Australia, www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html
[6]. http://cis-india.org/internet-governance/publications/privacyapproachpaper
[7]. https://www.aclusandiego.org/wp-content/uploads/2012/03/Social-Networking-Rights-teens.pdf
[8]. https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013#cite_ref-http:.2F.2Fperry4law.org.2Fcecsrdi.2F.3Fp.3D1128_6-0
[9]. http://www.constitution.org/cons/india/p03019.html, 15 April-2017