INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES

www.scienceandnature.org

PRIVACY AND SECURITY OF ELECTRONIC COMMUNICATION IN INDIA: A SOCIO-LEGAL STUDY

Arunava Narayan Mukherjee
Associate Professor(Human Resource Management)
Institute of Management and Information Science, Bhubaneswar, India

ABSTRACT

In to-day's gradually evolving sustainable knowledge society, or synonymously sustainable information society, knowledge or information has turned out to be one of the most valuable assets that are causing profound societal transformations all around the globe – a process that can justly be called globalization. However, at the basis of historical evolution of this new social formation - rise of sustainable knowledge/information society – lies the important driving force – the Information and Communication Technologies (ICTs). The social processes of globalization driven, *inter alia*, by the ICTs in a very important sense, are not only metamorphosing the world into a global village but also shaping all the sectors of human activity including production, dissemination or protection of knowledge and information in the domain of science and technology. The intellectual property rights of various kinds are undergoing revision and redefinition in the light of globalization of the different societal components – economic, political, cultural or social – at the global, regional, national and local levels.

Against this background the present paper endeavors to analyze the different issues of the privacy and security dimensions of the ICTs inasmuch as they bear on the Indian society including especially its electronic communication system, which is usually the medium and container of a country's 'intellectual capital and knowledge bank. It undertakes a brief review of the relevant socio-legal literature and narrates how the ICTs are are affecting social experience and research and development in globalizing India. And in this particular context the proposed paper shows how significant the privacy and security aspects of electronic communication have become and how the ICTs can promote freedom for the individual or become a source of cyber crimes affecting the society. The present paper achieves this objective by analyzing the relevant legal literature and case laws including, among other things, the Information Technology Act of 2000 and draws attention to how the privacy and security aspects of electronic communication in India are maintained in real life, and what the prevailing practices are in this connection. This is supplemented by a discussion of some suggestions that may diminish the cyber-dangers, protect the privacy and security, and thus promote the expansion of science and technology in Indian society.

Key words: Information and Communication Technology (ICT), Electronic Communication, cyber crime, The Information Technology Act of 2000, VSNL

INTRODUCTION

Electronic communication is a generic term which referrers to all the aspects of internet and World Wide Web. Internet is the world's largest computer network, originally started in USA for defence purpose. Now a days, from exchange of information to business transaction almost every form of human interaction and communication is carried out through net. This paperless electronic digital technology based communication system has transformed the life of human beings. Unlike the traditional form of communication, through Internet information can be exchanged in a collaborative manner, visually and audibly. It has made a "revolution" so far the concepts of time, distance and space in communication system, are concerned. Today we are traveling on the information superhighway of a global village, where data transfer and communication is virtually instantaneous.

Security aspect of Electronic Communication in simple words mean or imply all the information contained and communicated through this medium are duly protected, the potential vulnerabilities of this communication system are in the process of identification and elimination and development of necessary frame work of measures to respond to the threats and risk of fast changing digitally enabled environment. In India this particular issue came to limelight with the arrival of Internet.

Let us start with a classic example of flagrant violation of cyber security system in India. It was at the end of 1990s. With the wake of globalization the electronic frontiers were opening up in India. It was a virgin territory married to no law and regulation. As head of India's largest Internet service provider VSNL Amitabh Kumar used to surf the Net to see what's new. But one fine morning he was shocked to see a detailed notification, purportedly from his own company, VSNL, announcing a drastic slash in Internet charges. It was worse to see the message was in his own

name. Kumar had been hacked. Hacking is the electronic version of a break-in. And surprisingly this happened after a new Sun 04 security system had just been installed in VSNL'S computer banks to prevent hackers from breaking in. Later on it was detected, the culprit was a college student from Bangalore.

After that about a decade has passed. In this period India witnessed a galloping pace of economic liberalization, social change, World Wide Web connectivity. This October, electronic mail was sent from misleading Email address, threatening to assassinate Prime Minister Dr. Manmohan Singh when he will visit Kerala on 1st November. Security Agencies geared up and swung into action. With the assistance from Microsoft of US they could detect the alpha numeric code that the sender used to sign off his email and eventually arrested the miscreant, a 26-year-old computer hardware instructor employed in Ernakulam, Kerala.

The above mentioned incidents only go on establishing the fact, over the years, the security aspect of electronic communication in India is becoming a major issue in public life to reckon with. Like other parts of the World, in India also, cyber crime is gradually becoming a common antisocial phenomenon. The illegal activities committed, violating security of electronic communication in India constitute crimes in which the computer itself or the stored information is the target. According to Sankar Sen former Director National Police Academy, India. Criminal groups who view computers as target have been placed in three categories, (1) hackers, (2) those who break the systems to intentionally cause harm or mischief to data or .programs, and (3) financially motivated offenders who use a "specialized skill" to steal or damage information contained in computer storage.

Now we will examine the techniques of committing the crimes. The fastest growing computer related crime is theft, and the most common object stolen is information. Thieves very often target intellectual properties which include things like a new product patent, new product descriptions, market program plans, a list of customers and similar information. Previously the means to obtain these properties illegally where through employees, photocopying documents and burglaries, etc. Now the modus operandi has changed and thieves prefer stealing from the computers because it provides extensive access to more usable information. Many financial institutions receive threats from the cyber terrorists to penetrate their computer systems and leave-messages threatening to destroy them unless they receive huge sums of money. Many banks round the world have been victimized and paid millions of dollars as extortion money to keep the system intact. Criminals use various devices that can send a destructive wind through the system. Cyber terrorism is becoming a matter of serious concern and exposes national security systems, banking or communication networks, financial and commercial transactions to grave dangers. Techniques for perpetration of computer crimes have also produced a new set of terminologies. Some of these are "Trojan Horse" a set of unauthorized computer instruction which perform an illegal act a certain time or under certain conditions "Trapdoor "- a set of computer instructions that allow the user to bypass the system's normal controls; "Masquerading"- using a legitimate resource identification number to gain access to a computer system.

Privacy is another important aspect of electronic communication. There is no privacy law in our country. The Indian case laws explains "right to privacy" as the right which an owner of a house have to seclusion of his inner apartments from the view of his neighbor under local custom. The Supreme Court of India has declared the right to privacy as an integral part of the fundamental right to life under Art 21 of the Constitution of India. But that protection is only available against the state and fundamental rights can be curtailed by way of imposing reasonable restrictions. Therefore it is essential to be careful about the privacy on the net. An employer has no right to snoop over the emails sent by employees even from official mail account. However the reporting of misuse of official mail account is a good ground to monitor or vigil emails of employees.

The law specifies the company has the right to monitor the use of all its resources to ensure their proper utilization. But the law also says that in course of monitoring the employees must be informed. Generally here lies the point of conflict. In a Delhi-based MNC where the IT personnel were told to monitor IT usage and for this purpose they installed software. Without knowing this, one day when a senior unmarried executive was browsing through some abortion sites and the systems personnel were alerted. Very soon the news spread allover the office and the humiliated woman thought this was a violation of her privacy; so she took the company to court. The company can examine Internet usage of its employees, but they must be informed about it.

THE GENESIS AND GROWTH

Internet is a worldwide network of thousands of computer. The Internet started in the USA in a small way in 1969 as an experiment by the United States Department of Defence ("DOD"), to link DOD with military research contractors. It started from three computers in California and one in Utah. Gradually the Internet became a revolutionary phenomenon in the nineties when it moved out of the research institutes into the residence of common people across the world. People use Internet for sending and receiving e-mail, voice telephony, chatting and making friends, business through e-commerce, group discussions, access to information, and multimedia communication. The Internet provides an inexpensive and information rich, shared network interconnecting a large number of people and computers across the world. According to a recent estimate the current size of the Internet is 250 TB (terabytes) and is growing at an annual rate of 60%. The number of Internet users around the world is estimated at about 200 million at present but growing @80% per annum. Around the world, the growth in users, nodes and servers will certainly lead to a virtual information explosion. The quantity of data will witness an exponential growth. The quality of the data will also become more sophisticated including rich content consisting of voice

and data and graphics. The popularity of Internet can be understood from the fact that Internet became a mass media within five years of its launch whereas for radio it took 30 years. Internet reached to 100 million in just five years (Note: A media becomes a mass media when it reaches 50 million people). Internet is defining the way we communicate with each other, live, play, work and conduct business. It is challenging the established norms of doing day to day business. Today, a person just need a computer a browser and can access to the Internet and the world is in his fingertips. The recent development of Wireless Application Protocol (WAP) promises to make the Internet mobile i.e. it is accessible through the cell phones and can browse the WAP enabled sites.

THE INDIAN OPERATION

The Internet which came to India in 1 985 with the educational and research Network (ERNET) project of the Department of Electronics, Government of India was initially made available to IITs which gradually extended to other research and educational institutions. In the month of August 1995, Videsh Sanchar Nigam Ltd. (VSNL), a Public Sector Undertaking, started offering Internet service to common people. This opened up unexplored market. It was realized by the government that a single international gateway access provider like VSNL would not be able to handle the growth in Internet traffic in information super highway and keep in pace with the technological innovations and changes. Obviously there would be problems of: Congestion, Quality and Service. The government therefore on the basis of the recommendation of the IT Task Force decided to open up the net to private sector i.e. privatization of ISP or Internet services were thrown open to private sector in 1998. The Internet Service Providers in India include :

- VSNL - the undisputed leaders with over 70%.
- MTNL - the second govt. controlled agency with similar tariffs like VSNLI.
- Satyam Info - the first private ISP in India.
- Bharti BT - the first private ISP with international gateway.
- Dishnet Dial (formerly ETH).

The privatization has lead to increase in competition, which will ultimately pave way for lower tariff, more sophisticated products and services such as E-Commerce.

REVIEW OF RELEVANT LITERATURE

The literature on this topic can be broadly classified into three categories. The first category generally deals with the technical aspect of security and privacy of Electronic Communication. Under this category comes works like **Fundamentals of Computer Security Technology by E. G. Amoroso, 1994, Englewood Cliffs, N. J.: PTR Prentice Hall. xxii, 404 ; The Computer Privacy Handbook by A. Bacard, 1995, Berkeley, Calif.: Peachpit Press. xii, 274 ; Computer Security: Threats and Countermeasures by K. N. Bhaskar, 1993, Manchester: NCC Blackwell. xv, 357 ; Digital Crime: Policing the Cybernation by N. Barrett, 1997, London: Kogan Page. 224 ; Network and Internet Security by V. Ahuja, 1996, Boston: AP Professional. xix, 324 ; Security Issues for the Internet and World Wide Web by D. Cameron, 1st ed. 1996, Charleston, S.C.: Computer Technology Research. viii, 218 ; Computer Communications Security: Principles Standard Protocols and Techniques by W. Ford, 1994, Englewood Cliffs, N.J.: PTR Prentice Hall. xxii, 494 .**

Second category deals with the security and privacy aspect in the field of electronic commerce and governance. The important work are **Web Security and Commerce by S. Garfinkel and G. Spafford, 1997, Sebastopol Ca., O'Reilly ; Business in the Information Age: Heading for New Processes by H. Osterle, 1995, Berlin, New York: Springer. xvi, 387 ; Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption by W. Ford and M. S. Baum, 1997, Upper Saddle River, N.J.: Prentice Hall PTR. xxv, 301 ; The World Wide Web: Strategies and Opportunities for Business by D. Cameron, 1st ed. 1996, Charleston, S.C.: Computer Technology Research. ix, 239 ; E-commerce Security: Weak Links, Best Defences by A. K. Ghosh, 1998, New York: John Wiley. xv, 288 .**

And the third category is concerned with the socio-legal implications of electronic communication. The important works are **E-security and You by Sundeep Oberoi, 2001, New Delhi: Tata McGraw-Hill ; Social Engineering: Techniques and Preventions by S. Gordon, 1995, Compsec Conference on Security, Audit and Control, London, Elsevier, 445-50 ; Capital, Technology and Labor in the New Global Economy by A. F. Burns, J. H. K. Singh and S. L. Husted, AEI studies,480. 1988, Washington D.C.: American Enterprise Institute for Public Policy Research. xxvii, 203 ; Legislating Privacy: Technology Social Values and Public Policy by P. M. Regan, 1995, Chapel Hill: University of North Carolina Press. xix, 310 ; Making the Internet Family Friendly by B. Lang and B. Wilson, 1999, Nashville, Tenn.: T. Nelson. 180 ; The Information Game: Ethical Issues in a Microchip World, Studies in Applied Philosophy by G. Brown, 1990, Atlantic Highlands, N.J.: Humanities Press International. ix, 163 ; After the Death of Childhood: Growing Up in the Age of Electronic Media by D. Buckingham, 2000, Polity Press, Cambridge ; Technology: The Surrender of Culture to Technology by N. Postman, 1992, Knopf, New York, NY .**

THE EXISTING LEGAL FRAMEWORK

The Background

New communication systems and digital technology has made dramatic changes in our life. There is a remarkable change in the process of business transaction. Businessmen are increasingly using computers to create, transmit and store information in the electronic form instead of traditional

paper documents. It is cheaper, easier to store, preserve and retrieve and speedier to communicate. Although people are aware of these advantages they are not inclined to conduct business in the electronic form due to lack of appropriate legal framework. The two major hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements for legal recognition of writing and signature. At present many laws assume the existence of paper based records and documents which must bear signatures. The Law of Evidence is based upon conventional and traditional paper-based records and oral testimony. Electronic commerce does not require paper-based documents and paper-based transactions. Therefore for the purpose of facilitating e-commerce, proper legal frameworks become a necessity.

Governmental initiative

Government has rightly realized the need for introduction of a new law and for making suitable and necessary amendments to the existing laws to facilitate e-commerce and give legal recognition to electronic records and digital signature. The legal recognition accorded to electronic records and digital signature in turn will facilitate the conclusion of contracts and make the creation of legal rights and obligations possible through the electronic medium like internet. Ministry of commerce first drafted the Electronic commerce Act. Then it drafted the Electronic commerce support Act. Subsequently the Department of Electronics prepared the information Technology Bill. As per the requirement of Entry-26 of the state list in the 7th schedule to the constitution, the state Government has to frame laws to administer trade and commerce within the state. Accordingly, Central Government has circulated the draft legislation on Information Technology to all the State Governments seeking their views. They have extended their support to the legislation and have also expressed urgency for such legislation. Central Government placed the Information Technology Bill, 1999 (Bill No. 135 of 1999) in the Lok Sabha on 16.12.1999. The Lok Sabha passed the Bill on 16.5.2000 and Rajya Sabha passed it on 17.5.2000 by voice vote. The Bill has been assented by President on 9.6.2000 as Act No 21 of 2000. A few countries have enacted Cyber Laws and India is the second Asian country to codify a cyber law.

A panel of 5 members headed by Jayakrishnan, Secretary, Ministry of Information Technology, is entrusted with the assignment of drafting the Rules and Regulations.

Salient Features of the Act :

1. Data, electronic forms and electronic records get legal recognition. They are now admissible as evidence like paper based documents.
2. The Bill accords legal recognition to the system of digital signatures. Digital signatures performs the duty of regular signature, in other words, Digital Signature has become equivalent to regular signature. Government will prescribe rules for affixing digital signature.
3. Applications and documents can be filed with Government in electronic form.
4. Government gazette can also be published in electronic form.
5. By virtue of the Act regulatory authorities viz. Controller and Certifying Authorities are created who are empowered to deal with various issues associated with E-Commerce transactions.
6. Government to form Cyber Regulations Advisory Committed who shall provide policy guidelines to the Government and the Controller.
7. Various computer crimes have been defined and penalties provided for infringement of Cyber laws.
8. Hacking with computer system is an offence punishable with imprisonment up to 3 years and with fine up to Rs. 2 lacs.
9. Government will appoint Adjudicating Officers to enquire into computer related crimes and award compensation.
10. Government will establish a Cyber Regulation Appellate Tribunal to hear appeals against orders passed by Adjudicating Officers.
11. Controller and Adjudicating Officers are empowered compound the offences against the Act.
12. Police Officer not below the rank of DSP can conduct raid and arrest people without warrant for suspected cyber crime.

EVALUATION OF THE ACT

Although IT Act 2000 is a significant step in the field of Electronic communication in India, it is not free of criticism. We will try to analyze the success and shortcomings of the Act in the following manner.

Achievements of the Act

(i) The act made a pioneering contribution by way of giving legal reorganization and Validity to the transactions carried through the electronic medium. The operation of the Act facilitated the process of carrying out electronic commerce on the basis of a legal and administrative foundation.

(ii) The act not only recognizes electronic records and digital signatures but it also provides evidential value to online contracts.

(iii) It also permits electronic filing of documents and forms to government agencies.

In nutshell, it offers a legal mechanism to execute electronic commerce and electronic governance, while attempting to manage and control cyber crime.

Shortcomings of the Act :

(i) Although the Act recognizes the electronic document and digital signatures, (Sec. 6 & 7) but in surprising contradiction it does not confer any right on any

individual to insist that the particular document should be accept in electronic form. The goal of the Act is to pave the way for electronic communication on a legal footing, not to create hindrances by way of introducing and practicing "Redtapisum".

(ii) The Act does not exhaustively deal with the issue of "Cyber squatting" or stealing the domain name from it legal owners and intellectual property rights of the owner. Moreover, issues like patent, trade mark Copyright remains unaddressed.

(iii) The procedure of adjudication (of persons who acted in contravention of the Act) has not been defined and explained in the Act that too specially for those case where the offence has been committed beyond the territory India.

(iv) The Act empowers the government and its agencies to intercept any information transmitted through computer resources, if it is necessary in national and public interest, in the interest of the security of the state and maintenance of public order. The champions of individuals liberty views it as a threat to individual freedom and privacy and feels there is every probability to misuse this section for vested and political interest by the government in power.

(v) Under the Act, the authority of Central Government in appointing any person as Presiding officer of a Cyber Appellate Tribunal cannot called in question and no Act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely on any defect in the constitution of Cyber Appellate Tribunal. This provision goes against the spirit of fundamental rights of citizens (chapter III of Indian Constitutions) and therefore contradicts the highest law of land.

(vi) Besides, there are certain areas which have not been addressed by the Act such as controlling the conduct of cyber cafes; net pornography hosted web sites of foreign origin; taxation of e-commerce transactions; spamming or the sending of unsolicited commercial emails that amounts to breach of individuals' right to privacy on the net; crimes committed by web sites of foreign origin; etc.

(vii) The Act has vested police with unlimited and unrestricted power. Section 80 of the act says an officer not below the rank of Deputy Superintendent of Police (DSP) can enter any public place, search and arrest any person found there, without any warrant who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act. In Indian context there is all possibility of this unchecked power being misused, reminding us the classic precept "absolute power corrupts absolutely".

SECURITY ENVIRONMENT IN ELECTRONIC COMMUNICATION

Understanding the Practice:

Evolution of the concept of security in Electronic communication :

During the pre internet, pre LAN, WAN stage security and privacy confined to maintaining the confidentiality of the information by the concerned person or organization who is in possession of it. The control was on the access of the information. Selective information was available only to certain number of people. With the coming on internet, a new dimension was added to the concept of security. The attacks on security come in the form of worms, virus and websites containing hacking programs to aggress internet servers and mails. To combat these threats Antivirus and firewalls were introduced consecutively.

In the next phase the objective of the attack was not only to break in to some one's system through internet but to make undue financial gain out of it, taking advantage of the process of electronic commerce carried out in the era of open globalize business and economy. Naturally to thwart this aggression new instruments like digital signature, virtual private network etc were introduced.

In the present juncture it has been understood, not only technology but process and people also play a very important role to maintain the security and privacy of electronic communication. This point can be elucidated best by giving recent examples from the Indian BPO Industry which is an IT enable sector. The "sting operation" broadcast by a British T.V. channel just a few months back this year shows a young engineer from Kolkata admitting, he has stolen credit card related confidential information of customer while working in a BPO. Such incidents occurred in recent past in New Delhi, Pune and other parts of the country quiet frequently compelling NASSCOM to announce the proposition of introducing a National Employee Registry, which will help to keep a track of the employees working in BPO sector which in turn shall ultimately help to maintain the information security of the BPO industry.

Risk Areas and Vulnerability of information in Electronic Communication :

There are certain causes which are responsible for generation of risk. One of the primary causes is inherent factors embedded in the communication process like strategy, location, structure etc. Some risks are generated out of functional errors such as human/manual errors (mistake in data entry operation), improper handling of IT instruments, etc. Besides now a days a major risk is caused by none other than human beings who are known as "social

engineers" in the fields of electronic communication, who use the confidence tricks and other devious methods to persuade people to divulge sensitive information such as password or individual personal record.

The above mentioned risk areas create following types of vulnerability of information :

i) Observing the information by or exposure of information to unauthorized persons, without the knowledge and permission of the owner of information.
ii) Destruction of information or a database deliberately, accidentally or unintentionally and as a result of natural devastation or disaster, leading to denial of access to information.
iii) Taking away or copying information without knowledge of owner illegally or unauthorized manner.
iv) In case of electronic communication information and data is recorded through technology and available in "Cyber or Electronic form" rather in "Physical form".

Therefore even any trivial change intentional or accidental shall result in denial of access to or destruction of information.

Mechanism to Combat Threats on Security and Privacy:

Process

While designing the process of electronic system following aspects are to be taken into consideration in order to thwart attack on security system :

- **Confidentiality:** It refers to the assurance that information is divulged only to the intended recipients of the information.
- **Integrity:** It refers to the conformation that information has not been tampered with in an inadvertent or unauthorized manner.
- **Non-repudiation:** It refers to the assurance that neither the sender or recipient of information can deny the act of sending and receiving the information in question.
- **Authentication:** It refers to the process that are required to ensure that the identity of any entity wishing to use an information resource is actually what is claimed to be.
- **Access control:** It refers to the mechanism that ensures that any entity can only access those resources that it is entitled for using.
- **Availability:** It refers to the assurance that information resources will be available whenever required. With the development of networking system, availability has been recognized as a very important security issue.

Besides, to make the process of electronic communication security proof due emphasis should be given on survivability of the system, identifying, evaluating and protecting key information and for that matter classifying valuable information, maintenance of proper standards of security.

Technological

- Antivirus or Virus scanning software.
- **Firewall:** It is a mechanism comprising of both hardware and software which separates a private network from the public network.
- **Security Audit:** It is a thorough evaluation and appraisal of various aspects of web security of an organizations specially of its website and taking necessary actions of the basis of the review.
- **Intrusion Detection System**: With the help of the system an organization is able to make an analysis of real time data and to detect and prevent unauthorized network access.
- **Biometric Device:** In this process physical attributes of human being are used as a basis for automated identification.
- **VPN:** It is a device which ensures the authentication of data and application during their exposure to various users.
- **Secure Socket Layer Protocol:** During data transmission over Internet through this mechanism encryption of data is done between the browser on the customer's computer and the software on the Web Server.

Other available tools are Content Vectoring Protocol used for the purpose of scanning files for virus, Public Key Infrastructure for verifying the authentication of transmitted message, RSA token to ensure the security of the system with multiple login, Solutions for data backup namely SAN Technology etc.

Human

Security to a great extent is a matter of human perception. If one has got right perception about it and acts accordingly, less are the threats on security. In case of any security system awareness and security mindedness of the people who are associated with it are essential as in the case of cyber security. Even the most sophisticated Technology can not ensure safety and security of data and information unless the human factor involved is taken care of. Professionals and common people both are to be educated about the value of information in cyber communication and how to protect it.

The Indian Experience :

Electronic communication system is here to play a very important role in the development of our country. It will be possible provided the socioeconomic realties of the land are taken in to consideration while administrating this system. It must be designed to fulfill our indigenous requirements. In the following paragraphs we will discus during the use of electronic communication system in India, how its security and privacy has been provided by various corners, and what are the future strategies.

Indian corporate sector, specially those industries which are in to IT enabled services under the leadership and guidance of NASSCOM try to maintain global security standard like BS 7799 certification, SAS70 audit, etc.

NASSCOM has under taken thorough and comprehensive programs on the security environment and practices in India, emphasizing on following areas:

A) **Network security**: Under this segment it is verified whether Indian companies have security mechanism like anti-virus, firewalls at different levels, methodologies authentication and access control, encryption, VPN, Instruction Detection System etc.
B) **Physical security:** It covers deployment of security personal, fire management coping with other exigencies, introduction of sophisticated system like biometric access control etc.
C) **Personal security:** It ensures maintenance of confidentiality and compliance of nondisclosure agreement by employees of the organization, screening their background and educating them and providing them training on security management.
D) **Business continuity & disaster recovery:** It ensures whether companies have definite plans and strategies in this connection, and plans to manage contingency at site.

BPO companies also ensure compliance with global security standards like OCC regulation for banking, GLBA for financial services, HIPAA for healthcare services etc. "4E" frame work has been developed by NASSCOM for making India a safe destination where business process can be outsourced without risk. Following is the elucidation of "4E" mechanism:

4E stands for four junctions – engage, educate, enact and enforce. Engage means engagement of national and international advisory bodies on security and meeting stake holders of India and other important markets. Educate signifies workshops and symposium for members of legislature and judiciary and other concerned persons to make them aware about cyber security and preparing reports on security functions, standards, moral, contracts, legislation etc. Enact stands for investigating of various areas of cyber security to solidify the legal frameworks and thereby to introduce effective security practices. Enforce implies application of the mechanism created specially to ensure cyber security.

Although issues like unauthorized access to computer system or networks, hacking, security aspect of digital signature have been taken care of by IT Act 2000 and certain matters relating to operational and physical security has been elaborately delft in IT (certifying authorities) rules 2000 and IT security guidelines, the main objective of IT Act 2000 perse is to accord legal recognition to "electronic commerce". And this objective itself does not speak for the coverage of all security related aspects.

It is true under the initiative of government and NASSCOM law enforcing mechanism is gearing up to ensure cyber security. Central bureau of investigation formed cyber crime investigation cell (CCIC) in the year 2000 which is having all India jurisdiction. It investigates offences committed under IT ACT and other crimes committed with the help of high technology. The CCIC is the member of Interpol. Working party on information technology crime for South East Asia and Australia. Police department of different states and metropolitan cities in India has set up similar units. Mumbai cyber lab a joint venture of NASSCOM and Mumbai police has been setup to make common people aware about cyber security and to provide necessary guidance in this connection.

The National Police Academy, Hyderabad has been directed by the Central Government for preparing a handbook on "procedure to handle and use digital evidence in the cases of cyber crime". The idea of having an Electronic Research and Development Centre to design and develop cyber forensic tools is under the active consideration of government. India's intelligence bureau claims to have developed an E-mail investigation tool like America's Federal Bureau of Investigation Carnivore system. India and USA jointly launched a cyber security forum in 2002 and subsequently NASCOM and Information Technology Association of America jointly organized first Indo-US information security summit in 2004.

But still lot of cyber security related issues which affects public life remains unaddressed. The e-government system has been introduced without proper security infrastructure. Now a days, in financial sector "Internet Banking", "ATM" facility and means of cashless transaction like Debit card, Credit card, are very common and popular. But it is a matter of grave concern, an effective system has not yet been developed to monitor and ensure the techno-legal compliance mandatory to perform these activities.

Any form of system or process based on Electronic communication be e-governance or e-commerce, shall not be successful until we develop proper infrastructure for it and that exclusively depends on maintenance of security and privacy of the system. It is not an easy task. It involves the knowledge of both law and information technology. This calls for introduction of new disciplines like Cyber Criminology and Cyber Forensic to produce professionally skilled personnel who can aptly deal with problems of cyber security.

India deliberately needs a comprehensive data protection law regarding which ground work has already been started. Moreover the process to enact the law of convergence has already been initiated. The communication convergence bill 2001 was tabled in both House of Parliament and the standing committee on IT has already made its recommendations on the bill to the government. The object of the bill is to set up a super regulatory mechanism - The Communication Commission which will overview voice and data communications inclusive of Telecom, Broadcasting and Internet.

Finally keeping India's socio-economic conditions in mind it can be very conformingly said no initiative as discussed above can be effective without the awareness of common people who are the users of computers about cyber security and privacy. General awareness should be created keeping in pace with the development in the techno-legal areas of electronic communication.

OBSERVATION

In the present era of globalization along with opening up the economy, certain other inevitable changes took place in the socio cultural life of India. One of the major factors which affected change in Indian life simultaneously with the process of economic liberalization is the advent of electronic communication system. Since independence we lived in such a system where access and use of information was the monopoly of a certain section of people. In a socialistic bureaucratic set up, position of power determined accessibility to and availability of information. Electronic communication has revolutionized the conventional mode of communication and thereby made the process of procurement and utilization of information much easy, quick and effective. Outcomes of economic liberalization, to be more precise, market economy and consumerism have been instrumental in infusing material culture among Indian mass quite successfully. A generation has come up devoid of idealism, sense of social commitment, and sacrifice. Egotism and financial gain is the order of the day, which not only reigns over younger generation but has also taken into its fold an opportunist self centric community of people comprising of various age groups. But the eternal law of life gifts the youth with spirit of adventurism. In a complicated fast life where warmth of relationship is vanishing, having found no cause to champion and no ideal to follow certain section of them use electronic communication as a means to satisfy their desires for adventurism. In normal course the government and other systems which were impregnable so far can be "hacked" by using electronic communication and thereby they enjoy a unique sense of power. It is a challenge for them to break into an unbreakable system and to conquer it. They experience a sense of exhilaration of being illegal explorer. It's an unique electronic form of anti-establishment aggression.

There has been deviation from normal social behavior under the influence of electronic communication. In present technological environment young generation's need for social affiliation, recognition, friendship is determined in a significant manner by their possession and use of IT. Denial of access to IT virtually ostracizes them which clearly indicate their inability to socialize by way of normal human interaction. This is a sign of regimented behavior which impedes the development of personality, which might lead to antisocial tendencies and apathy towards society. This section of youth is not aware of the social skill of being accepted by other and accepting other at same time. Sense of true belongings and togetherness generate from direct human interaction, which can not be and should be at the mercy of information technology. IT should be used to intensify the human relationship, it should not become the only means to socialize.

Use of electronic communication has lead to typical polarization of the society. Certain section of people who are armed with the power to use and possess this medium of communication can be ascribed as "Technological Haves". Who do not use, possess and have access to this communication system can be called "Technological Have Nots". It is not the distribution of physical wealth but distribution of wealth of information and choice of communication that have divided the society. And if this gap is not bridged with the spread of IT education and systematic knowledge of use of IT, the growing social imbalance may cause various social problems in future.

Finally it can be said security and privacy is a matter of being aware and alert. Unless one is aware of the computer systems and alert about IT related dangers, with the best security system at his disposal, he shall fail. It is not the system of technology but human beings, who decide, determine and maintain the confidentiality of the information.

Therefore the Indian mass as well as law enforcing agencies have to be trained in the use and maintenance of confidentiality of data, so that they can have better perspective about security and privacy aspect of electronic communication.

Note:

This is the unrevised form of a paper presented in XXXII All India Sociological Conference 2006 at Loyola College, University of Madras with change of title. The data & information used in the paper correspond to the time of planning and drafting the paper (1999-2005), not based on current data & development.

ACKNOWLEDGEMENT

I gratefully acknowledge the valuable inputs especially on narrative analysis, knowledge of which I gathered from various course materials of DEC of **SIKKIM MANIPAL UNIVERSITY WHILE TEACHING THEM.**

REFERENCES AND SOURCES

[1] Referencer on e-commerce and information technology law – The Institute of Company Secretaries of India.

[2] Sen Sankar,(2000) "Cyber Crimes - Police Should Be Properly Equipped", The Statesman(Calcutta Edition) 11th September 2000.

[3] India Today "The Cyber Pirates" 12th April 1999.