SPEECH AT IST INTERNATIONAL CONFERENCE ON MANAGEMENT OF TECHNOLOGIES & INFORMATION SECURITY ORGANIZED BY THE IIIT ALLAHABAD ON 21.1.2010.

By

CHIEF GUEST

Justice Rajesh Tandon,
Chairperson,
Cyber Appellate Tribunal
Ministry of Communications & Information Technology
Department of Information Technology,
Jeevan Bharti (LIC) Building, Connaught Place
New Delhi.

I welcome Sh.M.D.Tiwari, Director, Sh.Abhishek Vaish, Co-Ordinator of IIIT,Allahabad and delegatees from the World, Prof.Alexandar Dimitriev from Moscow, Russia, Prof.Angappa Gunasekaran, from USA, Prof.Arun Jain from Buffalo, USA, Prof.Bharatendra K.Rai, from USA, Dr.C.Jayachandran, from Montclair State University, Dr.Deborah C.Hurst, from Canada, Prof.David Cobham, from UK, Prof. D.N.Talwar, fromUSA, Prof.Eugene Levner from Israel, Prof.Gerard McElwee, from UK, Prof.H.Raghav Rao, from USA, Prof.Marina Dabic, from Croatia, Dr.Pekka Kess, from Finland, Prof.Philip M.Tsang, from China, Prof. Reggie Kwan, from China, Prof.Roger Maull from UK, Prof.Satish Kumar Tripathi from USA, Prof.Satish Chandra, from USA, Prof.Sami Baboek, from Slovenia, Prof.Timothy Shea, from USA, Prof.Tugrul U.Daim, from USA, Dr.Vladimir Grigorievich Yakhno, from Russia and Prof. Vojko Potocan, from Slovenia.

It is a matter of pleasure that I am in the mids of the Technologists of the World. It is also a matter of pleasure that the IIIT has arranged the present Seminar.

Technology & Management which covers Technology and Real Estate, Technology in Global Financial Sector, Risk Management through Technology in Banking Sector and also Managing Global Business.

Apart from that Information & Network Security covers the Business Data Security, Data Networks, Computer Forensics, Cryptography & Digital Signature. Track III covers all the ideas behind Strategic Technology Management which covers leadership in network Organizations. Information Technology Strategy Management also covers E-Commerce Strategy. Information & Communication Technology

Applications in different Industries. Mitigation of climate change through enabling technologies.

We are in the world of digital technology and communication system which has brought a revolution through various technology facilitating the Ecommerce and electronic governance.

The Information Technology Act,2000 was introduced on 9th June,2000. Mitigation that has led to the introduction of the Information Technology Act,2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No.51 of 162 dated 30th January,1997 which has recommended that all the States should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication. The preamble of Act 21 of 2000 reads as under:

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act,1872, the Banker's Books Evidence Act,1891 and the Reserve Bank of India Act,1934 and for matters connected therewith or incidental thereto;

Whereas the General Assembly of the United Nations by resolution A/RES/51/162 dated 30th January,1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade law;

And whereas the said resolution recommends, inter alia, that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information."

Gradually the Act was amended on 5th February,2009 being the Amendment No.10 of 2009 which has introduced the world digital signature instead of electronic signature as provided under Chapter II of Section 3 of the Act. In Section 2, Clause (ha) was introduced after the word (h) which provides the Communication device. It reads as under:

"Communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;"

Thereafter the word "Computer" has also been defined which means any electronic, magnetic, optical or other high sped data processing device or system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

Computer network has also been defined in the new amendment which reads as under:-

"Computer network" means the interconnection of one or more computers or computer systems or communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter connection is continuously maintained;

By the new amendment Cyber café and Cyber security has also been introduced by virtue of clauses (na) and (nb) which read as under:-

Cyber café means any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public;

Cyber security means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

A new Section has been introduced as Section 70B regarding Indian Computer Emergency Response Team which defines as under:-

70B. Indian Computer Emergency Response Team to serve as national agency for incident response.

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security-

(a) Collection, analysis and dissemination of information on cyber incidents;
(b) Forecast and alerts of cyber security incidents;
(c) Emergency measures for handling cyber security incidents;
(d) Coordination of cyber incidents response activities;
(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1).

The Act has also introduced "asymmetric crypto system by virtue of clause (f) of Section 2 of the Act. Which provides a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

The Act has given legal recognition to the electronic records.

The Act thereafter provides Digital signature and Electronic signature.

The digital signature creation and verification process achieves the following legal requirement.

Signer authentication: A person's digital signature cannot be forged unless his private key is stolen. This means that if a digital signature can be verified by Sanya's public key, then it

must have been created by Sanya's private key. The digital signature verification process thus authenticates the identity of the signer.

Message authentication: A digital signature is based upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

Affirmative act: The process of digital signature creation requires the signer to use his private key (usually by entering a password). This overt act alerts the signer that he is initiating a transaction that may have legal consequences.

The Act provides as under:-

3. Authentication of electronic records.-

(1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

3A. Electronic signature.-

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purpose of this section any electronic signature or electronic authentication technique shall be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person.

(b) The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) Any alteration to the electronic signature made after affixing such signature is detectable;

(d) Ay alteration to the information made after its authentication y electronic signature is detectable; and

(e) It fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second schedule;

(5) Every notification issued under sub section (4) shall be laid before each House of Parliament.

The Act also has introduced the Controller, Deputy Controller and Assistant Controller for verifying the electronic signatures and there is recognition of foreign certifying authority as well.

The most important factor of the Information Technology Act is that the Adjudicating Authority has been formed under Section 46 of the Act which provides the power to adjudicate and award damages which does not exceed Rs.5 crores and the factors to be taken into account by the Adjudicating Officer, the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;, the amount of loss caused to any person as a result of the default and the repetitive nature of the default. Therefore, the appeal lies to the Appellate Tribunal. The offences which are covered under the Information Technology Act are as under:-

The offences under the Information Technology Act are as under:

(1)Tampering computer source documents. **Section 65**

(2)Hacking with Computer System
Data alteration **Section 66**.

(3) Punishment for sending offensive messages through communication service etc. Section 66A

(4) Punishment for dishonestly receiving stolen computer resource or communication device. Section 66B

(5) Punishment for identity theft. Section 66C

(6) Punishment for cheating by personation by using computer resource. Section 66D

(7) Punishment for violation of privacy. Section 66E.
(8) Publishing obscene information . **Section 67**
(9) Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Section 67A

(10)Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. Section 67B
(11) Preservation and retention of information by Intermediaries. Section 67C

(12) Un-authorized access to protected system. **Section.70**
(13) Penalty for misrepresentation. Section 71
(14) Breach of Confidentiality and Privacy **Section 72**
(15) Punishment for disclosure of information in breach of lawful contract. Section 72A
(16) Publishing false Digital Signature Certificates. **Section 73**

It may also be pointed out that by virtue of Section 75, the Act has a legal world wide recognition even in respect of the offences committed out side as it is International Cyber crime Law.

Coming to the laws of the other States, US legal system, some of the US Legislation relevant to the cyber crime are to the following effect:-

1. No Electronic Theft Act. (1997).
2. The Digital Millennium Copyright Act.(1998)
3. The Child Online Protection Act (1998)
4. The U.S.Trademark Cyber piracy Prevention Act. (1999)
5. The Children's Internet Protection Act (2001) and
6. The USA Patriot Act (2001).

The No Electronic Theft Act was passed to amend the provisions of titles 17 and 18, United States Code and to provide greater copyright protection by amending criminal copyright infringement provisions. Prior to this law, people who intentionally distributed copied software over the Internet did not face criminal penalties if they did not profit from their actions.

Digital Millennium Copyright Act penalizes the circumvention of anti piracy measures built into software. It also makes it illegal to manufacture, sell, or distribute code-cracking devices used to illegally

copy software. Some of the exemptions provided by DMCA are cracking of copyright protection devices for conducting encryption research, assessing product interoperability, and testing computer security systems. Exemptions are also provided for nonprofit libraries, archieves, and educational institutions under certain circumstances. Internet service providers are exempted from copyright infringement liability for simply transmitting information over the Internet. They are required to remove material from users web sites that appears to constitute copyright infringement.

The Child Online Protection Act (1998). This law was enacted in view of Congressional findings to the effect that: the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control. This law prohibits knowingly using the World Wide Web for commercial communication of material to minors that is harmful for them.

The Children's Internet Protection Act relates to technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors. It provides requirements for schools and libraries to enforce internet safety policies with technology protection measures for computers with internet access as condition of universal service discounts. It also provides requirements for certain libraries with computers having internet access.

The primary purpose of The USA Patriot Act is to deter and punish terrorist acts in the United States and around the world and to enhance law enforcement investigatory tools.

Further there are laws to the effect of unauthorized access to the protected information and un-authorised access to financial information and un-authorised access of protected computers and further damages to the protected computers. Similarly under the Canadian law as well every person who (a) steals a credit card, (b) forges or falsifies a credit card, (c) possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered (i) by the commission in Canada of an offence, or (ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence, or (d) uses a credit card knowing that it has been revoked or cancelled, is guilty of (e) an indictable offence and is liable to imprisonment for a term not exceeding ten years, or (f) an offence punishable on summary conviction.

Under the Singapore law, for the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorized or done without authority if-

(a) he is not himself entitled to control access of the kind in question to the programe or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

Under the UK law, a person is guilty of an offence if-

(a) he does any unauthorized act in relation to a computer.

(b) At the time when he does the act he knows that it is unauthorized, and

(c) Either subsection (2) or sub section (3) below applies.

(2) This subsection applies if the person intends by doing the act-

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer.

(c) To impair the operation of any such program or the reliability of any such data; or

(d) To enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4)The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section-

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

However, the need is for a world wide law on the Cyber, world wide forensic lab, world wide data protection system and the cyber forensic which involves tracking soft ware piracy, recovering deleted data, preserving digital evidence for production in court and International code is required. I hope and trust that the delegatee present from all over world will soon organize conference at their level at their States in order to analyse the judicial procedure adopted by various States in relation to the International Cyber crime.