Cyber Laws in India

Objectives: This chapter presents the meaning and definition of cyber crime, the legislation in India dealing with offences relating to the use of or concerned with the abuse of computers or other electronic gadgets. The Information Technology Act 2000 and the I.T. Amendment Act 2008 have been dealt with in detail and other legislations dealing with electronic offences have been discussed in brief.

Introduction:

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.

Crime in any form adversely affects all the members of the society. In developing economies, cyber crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some one's mobile will tantamount to dumping one in solitary confinement!

Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber crime, about which we will now be discussing in detail.

In a cyber crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber crime.

Let us now discuss in detail, the Information Technology Act -2000 and the I.T. Amendment Act 2008 in general and with particular reference to banking and financial sector related transactions. Before going into the section-wise or chapter-wise description of various provisions of the Act, let us discuss the history behind such a legislation in India, the circumstances under which the Act was passed and the purpose or objectives in passing it.

The Genesis of IT legislation in India: Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

Objectives of I.T. legislation in India: . It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself.

"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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.

The Act essentially deals with the following issues:

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

Amendment Act 2008: Being the first legislation in the nation on technology, computers and e-commerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

- Focussing on data privacy
- Focussing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

In this chapter, we will be broadly discussing the various provisions of ITA 2000 and wherever the same has been amended or a new section added as per the ITAA 2008, such remark will be made appropriately.

How the Act is structured: The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the ITA 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from thereon the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc.

Elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and since replaced by electronic signatures in the ITAA -2008) have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described.

Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011. *We will be discussing some of the important provisions of such rules also in the later part of this chapter.*

Applicability: The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (ie where it is not applicable) as detailed in the First Schedule, stated below:

a) negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
c) a trust as defined in section 3 of the Indian Trusts Act, 1882
d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
e) any contract for the sale or conveyance of immovable property or any interest in such property;
f) any such class of documents or transactions as may be notified by the Central Government

Definitions: The ITA-2000 defines many important words used in common computer parlance like 'access', 'computer resource', 'computer system', 'communication device', 'data', 'information', 'security procedure' etc. The definition of the word 'computer' itself assumes significance here.

'Computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions 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;

So is the word 'computer system' which means a device or a collection of devices with input, output and storage capabilities. Interestingly, the word 'computer' and 'computer system' have been so widely defined to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities. A careful reading of the words will make one understand that a high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

Similarly the word 'communication devices' inserted in the ITAA-2008 has been given an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPad or other similar devices on Wi-fi and cellular models. Definitions for some words like 'cyber café' were also later incorporated in the ITAA 2008 when 'Indian Computer response Emergency Team' was included.

Digital Signature: 'Electronic signature' was defined in the ITAA -2008 whereas the earlier ITA -2000 covered in detail about digital signature, defining it and elaborating the procedure to obtain the digital signature certificate and giving it legal validity. Digital signature was defined in the ITA -2000 as "authentication of electronic record" as per procedure laid down in Section 3 and Section 3 discussed the use of asymmetric crypto system and the use of Public Key Infrastructure and hash function etc. This was later criticized to be technology dependent ie., relying on the specific technology of asymmetric crypto system and the hash function generating a pair of public and private key authentication etc.

Thus Section 3 which was originally "Digital Signature" was later renamed as "Digital Signature and **Electronic Signature**" in ITAA - 2008 thus introducing technological neutrality by adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as **one of the modes** of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone. While M/s. TCS, M/s. Safescript and M/s. MTNL are some of the digital signature certifying authorities in

India, IDRBT (Institute for Development of Research in Banking Technology – the research wing of RBI) is the Certifying Authorities (CA) for the Indian Banking and financial sector licensed by the Controller of Certifying Authorities, Government of India.

It is relevant to understand the meaning of digital signature (or electronic signature) here. It would be pertinent to note that electronic signature (or the earlier digital signature) as stipulated in the Act is NOT a digitized signature or a scanned signature. In fact, in electronic signature (or digital signature) there is no real signature by the person, in the conventional sense of the term. Electronic signature is not the process of storing ones signature or scanning ones signature and sending it in an electronic communication like email. It is a process of authentication of message using the procedure laid down in Section 3 of the Act.

The other forms of authentication that are simpler to use such as biometric based retina scanning etc can be quite useful in effective implementation of the Act. However, the Central Government has to evolve detailed procedures and increase awareness on the use of such systems among the public by putting in place the necessary tools and stipulating necessary conditions. Besides, duties of electronic signature certificate issuing authorities for bio-metric based authentication mechanisms have to be evolved and the necessary parameters have to be formulated to make it user-friendly and at the same time without compromising security.

e-Governance: Chapter III discusses Electronic governance issues and procedures and the legal recognition to electronic records is dealt with in detail in Section 4 followed by description of procedures on electronic records, storage and maintenance and according recognition to the validity of contracts formed through electronic means.

Procedures relating to electronic signatures and regulatory guidelines for certifying authorities have been laid down in the sections that follow.

Chapter IX dealing with Penalties, Compensation and Adjudication is a major significant step in the direction of combating data theft, claiming compensation, introduction of security practices etc discussed in Section 43, and which deserve detailed description.

Section 43 deals with penalties and compensation for damage to computer, computer system etc. This section is the first major and significant legislative step in India to combat the issue of data theft. The IT industry has for long been clamouring for a legislation in India to address the crime of data theft, just like physical theft or larceny of goods and commodities. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorised user or tampers etc…he shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008.

The essence of this Section is **civil liability.** Criminality in the offence of data theft is being separately dealt with later under Sections 65 and 66. Writing a virus program or spreading a virus mail, a bot, a Trojan or any other malware in a computer network or causing a Denial of Service Attack in a server will all come under this Section and attract civil liability by way of compensation. Under this Section, words like Computer Virus, Compute Contaminant, Computer database and Source Code are all described and defined.

Questions like the employees' liability in an organisation which is sued against for data theft or such offences and the amount of responsibility of the employer or the owner and the concept of due diligence were all debated in the first few years of ITA -2000 in court litigations like the bazee.com case and other cases**.** Subsequently need was felt for defining the corporate liability for data protection and information security at the corporate level was given a serious look.

Thus the new **Section 43-A** dealing with compensation for failure to protect data was introduced in the ITAA -2008. This is another watershed in the area of data protection especially at the corporate level. As per this Section, where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The Section further explains the phrase 'body corporate' and quite significantly the phrases 'reasonable security practices and procedures' and 'sensitive personal data or information'.

Thus the corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporates are under an obligation to ensure adoption of reasonable security practices. Further what is sensitive personal data has since been clarified by the central government vide its Notification dated 11 April 2011 giving the list of all such data which includes password, details of bank accounts or card details, medical records etc. After this notification, the IT industry in the nation including tech-savvy and widely technology-based banking and other sectors became suddenly aware of the responsibility of data protection and a general awareness increased on what is data privacy and what is the role of top management and the Information Security Department in organisations in ensuring data protection, especially while handling the customers' and other third party data.

Reasonable Security Practices

- Site certification
- Security initiatives
- Awareness Training
- Conformance to Standards, certification
- Policies and adherence to policies
- Policies like password policy, Access Control, email Policy etc
- Periodic monitoring and review.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules have since been notified by the Government of India, Dept of I.T. on 11 April 2011. Any body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies containing managerial, technical, operational and physical security control measures commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and

information security policies. The international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

In view of the foregoing, it has now become a major compliance issue on the part of not only IT companies but also those in the Banking and Financial Sector especially those banks with huge computerised operations dealing with public data and depending heavily on technology. In times of a litigation or any security breach resulting in a claim of compensation of financial loss amount or damages, it would be the huge responsibility on the part of those body corporate to prove that that said "Reasonable Security Practices and Procedures" were actually in place and all the steps mentioned in the Rules passed in April 2011 stated above, have been taken.

In the near future, this is one of the sections that is going to create much noise and be the subject of much debates in the event of litigations, like in re-defining the role of an employee, the responsibility of an employer or the top management in data protection and issues like the actual and vicarious responsibility, the actual and contributory negligence of all stake holders involved etc.

The issue has wider ramifications especially in the case of a **cloud computing** scenario (the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server, with the services managed by the provider sold on demand, for the amount of time used) where more and more organisations handle the data of others and the information is stored elsewhere and not in the owners' system. Possibly, more debates will emanate on the question of information owners vis a vis the information container and the information custodians and the Service Level Agreements of all parties involved will assume a greater significance.

Adjudication: Having dealt with civil offences, the Act then goes on to describe civil remedy to such offences in the form of adjudication without having to resort to the procedure of filing a complaint with the police or other investigating agencies. Adjudication powers and procedures have been elaborately laid down in Sections 46 and thereafter. The Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. If at all one section can be criticized to be absolutely lacking in popularity in the IT Act, it is this provision. In the first ten years of existence of the ITA, there have been only a very few applications made in the nation, that too in the major metros almost all of which are under different stages of judicial process and adjudications have been obtained in possibly less than five cases. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. in April 2010.

This section should be given much popularity and awareness should be spread among the public especially the victims of cyber crimes and data theft that such a procedure does exist without recourse to going to the police and filing a case. It is time the state spends some time and thought in enhancing awareness on the provision of adjudication for civil offences in cyber litigations like data theft etc so that the purpose for which such useful provisions have been made, are effectively utilized by the litigant public.

There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level, has also been described in the Act. Every adjudicating officer has the powers of a

civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure.

After discussing the procedures relating to appeals etc and the duties and powers of Cyber Appellate Tribunal, the Act moves to the actual criminal acts coming under the broader definition of cyber crimes. It would be pertinent to note that the Act only lists some of the cyber crimes, (without defining a cyber crime) and stipulates the punishments for such offences. The criminal provisions of the IT Act and those dealing with cognizable offences and criminal acts follow from Chapter IX titled "Offences"

Section 65: Tampering with source documents is dealt with under this section. Concealing, destroying, altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both. Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court (Bhim Sen Garg vs State of Rajasthan and others, 2006, Cri LJ, 3463, Raj 2411) attract punishment under this Section. Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc in any form.

Section 66: Computer related offences are dealt with under this Section. Data theft stated in Section 43 is referred to in this Section. Whereas it was a plain and simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Sec 66 and it was an offence.

Now after the amendment, data theft of Sec 43 is being referred to in Sec 66 by making this section more purposeful and the word 'hacking' is not used. The word 'hacking' was earlier called a crime in this Section and at the same time, courses on 'ethical hacking' were also taught academically. This led to an anomalous situation of people asking how an illegal activity be taught academically with a word 'ethical' prefixed to it. Then can there be training programmes, for instance, on "Ethical burglary", "Ethical Assault" etc say for courses on physical defence? This tricky situation was put an end to, by the ITAA when it re-phrased the Section 66 by mapping it with the civil liability of Section 43 and removing the word 'Hacking'. However the act of hacking is still certainly an offence as per this Section, though some experts interpret 'hacking' as generally for good purposes (obviously to facilitate naming of the courses as ethical hacking) and 'cracking' for illegal purposes. It would be relevant to note that the technology involved in both is the same and the act is the same, whereas in 'hacking' the owner's consent is obtained or assumed and the latter act 'cracking' is perceived to be an offence.

Thanks to ITAA, Section 66 is now a widened one with a list of offences as follows:

66A Sending offensive messages thro communication service, causing annoyance etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment upto three years or fine.

66B Dishonestly receiving stolen computer resource or communication device with punishment upto three years or one lakh rupees as fine or both.

66C Electronic signature or other identity theft like using others' password or electronic signature etc. Punishment is three years imprisonment or fine of one lakh rupees or both.

66D Cheating by personation using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.

66E Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.

66F Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or Trojan Horse or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. come under this Section. Punishment is life imprisonment.

It may be observed that all acts under S.66 are cognizable and non-bailable offences. Intention or the knowledge to cause wrongful loss to others ie the existence of criminal intention and the evil mind ie concept of *mens rea,* destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section.

To summarise, what was civil liability with entitlement for compensations and damages in Section 43, has been referred to here, if committed with criminal intent, making it a criminal liability attracting imprisonment and fine or both.

Section 67 deals with publishing or transmitting obscene material in electronic form. The earlier Section in ITA was later widened as per ITAA 2008 in which child pornography and retention of records by intermediaries were all included.

Publishing or transmitting obscene material in electronic form is dealt with here. Whoever publishes or transmits any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read the matter contained in it, shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

This Section is of historical importance since the landmark judgement in what is considered to be the first ever conviction under I.T. Act 2000 in India, was obtained in this Section in the famous case "State of Tamil Nadu vs Suhas Katti" on 5 November 2004. The strength of the Section and the reliability of electronic evidences were proved by the prosecution and conviction was brought about in this case, involving sending obscene message in the name of a married women amounting to cyber stalking, email spoofing and the criminal activity stated in this Section.

Section 67-A deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when combined with the material containing sexually explicit material attract penalty under this Section.

Child Pornography has been exclusively dealt with under Section 67B. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc or facilitating abusing children online or inducing children to online relationship with one or more children etc come under this Section. 'Children' means persons who have not completed 18 years of age, for the purpose of this Section. Punishment for the first conviction is imprisonment for a maximum of five years and fine of ten lakh rupees and in the event of subsequent conviction with imprisonment of seven years and fine of ten lakh rupees.

Bonafide heritage material being printed or distributed for the purpose of education or literature etc are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

Screening videographs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment upto three years or fine.

Transmission of electronic message and communication:

Section 69: This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here. This power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so.

Section 69A inserted in the ITAA, vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above. Section 69B discusses the power to authorise to monitor and collect traffic data or information through any computer resource.

Commentary on the powers to intercept, monitor and block websites: In short, under the conditions laid down in the Section, power to intercept, monitor or decrypt does exist. It would be interesting to trace the history of telephone tapping in India and the legislative provisions (or the lack of it?) in our nation and compare it with the powers mentioned here. Until the passage of this Section in the ITAA, phone tapping was governed by Clause 5(2) of the Indian Telegraph Act of 1885, which said that "On the occurrence of any public emergency, or in the interest of the public safety, the Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order". Other sections of the act mention that the government should formulate "precautions to be taken for preventing the improper interception or disclosure of messages". There have been many attempts, rather many requests, to formulate rules to govern the operation of Clause 5(2). But ever since 1885,

no government has formulated any such precautions, maybe for obvious reasons to retain the spying powers for almost a century.

A writ petition was filed in the Supreme Court in 1991 by the People's Union for Civil Liberties, challenging the constitutional validity of this Clause 5(2). The petition argued that it infringed the constitutional right to freedom of speech and expression and to life and personal liberty. In December 1996, the Supreme Court delivered its judgment, pointing out that "unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers" given them under 5(2). They went on to define them thus: a public emergency was the "prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action", and public safety "means the state or condition of freedom from danger or risk for the people at large". Without those two, however "necessary or expedient", it could not do so. Procedures for keeping such records and the layer of authorities etc were also stipulated.

Now, this **Section 69 of ITAA is far more intrusive** and more powerful than the above-cited provision of Indian Telegraph Act 1885. Under this ITAA Section, the nominated Government official will be able to listen in to all phone calls, read the SMSs and emails, and monitor the websites that one visited, subject to adherence to the prescribed procedures and without a warrant from a magistrate's order. In view of the foregoing, this Section was critizised to be draconian vesting the government with much more powers than required.

Having said this, we should not be oblivious to the fact that this power (of intercepting, monitoring and blocking) is something which the Government represented by the **Indian Computer Emergency Response Team, (the National Nodal Agency**, as nominated in Section 70B of ITAA) has very rarely exercised. Perhaps believing in the freedom of expression and having confidence in the self-regulative nature of the industry, the CERT-In has stated that these powers are very sparingly (and almost never) used by it.

Critical Information Infrastructure and Protected System have been discussed in Section 70. The Indian Computer Emergency Response Team (CERT-In) coming under the Ministry of Information and Technology, Government of India, has been designated as the National Nodal Agency for incident response. By virtue of this, CERT-In will perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc.

The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable. The Minister of State for Communications and IT Mr.Sachin Pilot said in a written reply to the Rajya Sabha said that (as reported in the Press), CERT-In has handled over 13,000 such incidents in 2011 compared to 8,266 incidents in 2009. CERT-In has observed that there is significant increase in the number of cyber security incidents in the country. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by CERT-In during 2009, 2010 and 2011, respectively," These security incidents include website intrusions, phishing, network probing, spread of malicious code like virus, worms and spam, he added. Hence the role of CERT-In is very crucial and there are much expectations from CERT In not just in giving out the alerts but in combating cyber crime, use the weapon of monitoring the web-traffic, intercepting and blocking the site, whenever so required and with due process of law.

Penalty for breach of confidentiality and privacy is discussed in Section 72 with the punishment being imprisonment for a term upto two years or a fine of one lakh rupees or both.

Considering the global nature of cyber crime and understanding the real time scenario of fraudster living in one part of the world and committing a data theft or DoS(Denial of Service)

kind of an attack or other cyber crime in an entirely different part of the world, Section 75 clearly states that the Act applies to offences or contravention committed outside India, if the contravention or the offence involves a computer or a computer network located in India.

This Act has over-riding provisions especially with regard to the regulations stipulated in the Code of Criminal Procedure. As per Section 78, notwithstanding anything contained in the Code of Criminal Procedure, a police officer not below the rank of an Inspector shall investigate an offence under this Act. Such powers were conferred to officers not below the rank of a Deputy Superintendent of Police earlier in the ITA which was later amended as Inspector in the ITAA.

Due Diligence: Liability of intermediaries and the concept of Due Diligence has been discussed in Section 79. As per this, intermediary shall not be liable for any third party information hosted by him, if his function is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or if he does not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission and if he observes due diligence and follows the guidelines prescribed by the Central Government.

This concept of due diligence is also much being debated. Due Diligence was first discussed as an immediate fallout of the famous bazee.com case in New Delhi, when the NRI CEO of the company was arrested for making the MMS clipping with objectionable obscene material depicting school children was made available in the public domain website owned by him, for sale (and later the CD was sold). The larger issue being discussed at that time was how far is the content provider responsible and how far the Internet Service Provider and what is due diligence which as the CEO of the company, he should have exercised.

After passage of the ITAA and the introduction of 'reasonable security practices and procedures' and the responsibility of body corporate as seen earlier in Section 43A, and to set at rest some confusion on the significance of due diligence and what constitutes due diligence, the DIT came out with a set of rules titled Information Technology (Intermediaries Guidelines) Rules on 11 April 2011. As per this, "the intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes….."

In essence, an intermediary shall be liable for any contravention of law committed by any user unless the Intermediary can prove that he has exercised due diligence and has not conspired or abetted in the act of criminality.

Power to enter, search etc has been described in Section 80. Notwithstanding anything contained in the Code of Criminal Procedure, any police officer, not below the rank of an Inspector or any other officer ….authorised ….may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit

any offence under this Act. This is another effective weapon that has been rarely and almost never utilised by the police officers.

The Act is applicable to electronic cheques and truncated cheques (ie the image of cheque being presented and processed curtailing and truncating the physical movement of the cheque from the collecting banker to the paying banker).

Overriding powers of the Act and the powers of Central Government to make rules and that of State Governments to make rules wherever necessary have been discussed in the Sections that follow.

Other Acts amended by the ITA:

The Indian Penal Code, 1860: Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.

ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (eg 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Indian Evidence Act 1872: This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

Admissibility of electronic records as evidence as enshrined in **Section 65B** of the Act assumes significance. This is **an elaborate section** and a landmark piece of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly .... by lawful persons.. (b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly ..... and .....a certificate signed by a person .....responsible..... etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section.

However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a Post Script remark at the bottom "This is a computer generated letter and hence does not require signature". The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

The Bankers' Books Evidence(BBE) Act 1891 Amendment to this Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended as: "'bankers

' books' include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry ...certified in accordance with the provisions ....to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons; the safeguards adopted to prevent and detect unauthorised change of data ...to retrieve data that is lost due to systemic failure or .....

In short, just like in the Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerised system with proper integrity of data, wherein data cannot be manipulated or accessed in an unauthorised manner or is not lost or tamperable due to system failure or such other reasons.

Here again, let us reiterate that the law **does not state** that any computerised print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE.

The next Act that was amended by the ITA is **the Reserve Bank of India Act, 1934**. Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through

electronic means between banks (ie transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

Observations on ITA and ITAA:

Having discussed in detail all the provisions of ITA and ITAA, let us now look at some of the broader areas of omissions and commissions in the Act and the general criticism the Acts have faced over the years.

Awareness: There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious step to create public awareness about the provisions in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. Especially, provisions like scope for adjudication process is never known to many including those in the investigating agencies.

Jurisdiction: This is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cyber crime etc. In the context of electronic record, Section 13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

However some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space', has to be spread and proper training is to be given to all concerned players in the field.

Evidences: Evidences are a major concern in cyber crimes. Pat of evidences is the 'crime scene' issues. In cyber crime, there is no cyber crime. We cannot mark a place nor a computer nor a network, nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Very often, nothing could be seen as a scene in cyber crime! The evidences, the data, the network and the related gadgets along with of course the log files and trail of events emanating or recorded in the system are actually the crime scene. While filing cases under IT Act, be it as a civil case in the adjudication process or a criminal complaint filed with the police, many often, evidences may lie in some system like the intermediaries' computers or some times in the opponent's computer system too. In all such cases, unless the police swing into action swiftly and seize the systems and capture the evidences, such vital evidences could be easily destroyed. In fact, if one knows that his computer is going to be seized, he would immediately go for destruction of evidences (formatting, removing the history, removing the cookies, changing the registry and user login set ups, reconfiguring the system files etc) since most of the computer history and log files are volatile in nature.

There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required. For this there are software tools like 'EnCase' wih a global recognition and our own C-DAC tools which are available with much retrieval facilities, search features without giving any room for further writing and preserving the original version with date stamp for production as evidence.

Non coverage of many crimes: While there are many legislations in not only many Western countries but also some smaller nations in the East, India has only one legislation -- the ITA and ITAA. Hence it is quite natural that many issues on cyber crimes and many crimes per se are left uncovered. Many cyber crimes like cyber squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Besides, most of the Indian corporate including some Public Sector undertakings use Operating Systems that are from the West especially the US and many software utilities and hardware items and sometimes firmware are from abroad. In such cases, the actual reach and import of IT Act Sections dealing with a utility software or a system software or an Operating System upgrade or update used for downloading the software utility, is to be specifically addressed, as otherwise a peculiar situation may come, when the user may not know whether the upgrade or the patch is getting downloaded or any spyware getting installed. The Act does not address the government's policy on keeping the backup of corporates including the PSUs and PSBs in our county or abroad and if kept abroad, the subjective legal jurisprudence on such software backups.

We find, as has been said earlier in the chapter, that most of the cyber crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of ITA or the ITAA which gives a comfort factor to the investigating agencies that even if the ITA part of the case is lost, the accused cannot escape from the IPC part.

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyberlaw and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ….. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world……"

Let us not be pessimistic that the existing legislation is cyber criminal friendly or paves the way to increase crimes. Certainly, it does not. It is a commendable piece of legislation, a landmark first step and a remarkable mile-stone in the technological growth of the nation. But let us not be complacent that the existing law would suffice. Let us remember that the criminals always go faster than the investigators and always try to be one step ahead in technology. After all, steganography was used in the Parliament Attack case to convey a one-line hidden message from one criminal to another which was a lesson for the investigators to know more about the technology of steganography. Similarly Satellite phones were used in the Mumbai attack case in November 2008 after which the investigators became aware of the technological perils of such gadgets, since until then, they were relying on cell phones and the directional tracking by the cell phone towers and Call Details Register entries only. Hopefully, more and more awareness campaign will take place and the government will be conscious of the path ahead to bring more and more legislations in place. Actually, bringing more legislations may just not be sufficient, because the conviction rate in Cyber crime offences is among the lowest in the nation, much lower than the rate in IPC and other offences. The government should be aware that it is not the severity of punishment that is a deterrent for the criminals, but it is the certainty of punishment. It is not the number of legislations in a society that should prevent crimes but it is the certainty of punishment that the legislation will bring.

Let us now discuss some of the other relevant legislations in the nation that deal with cyber crimes in various sectors.

Prevention of Money Laundering Act:

Black money has always been a serious evil in any developing economy. Nation builders, lawmakers and particularly the country's financial administrators have always taken persistent efforts to curb the evil of black money and all sorts of illegally earned income. A major initiative taken in this direction in India is the Anti Money Laundering Act 2002. A main objective of the Act was to provide for confiscation of property derived from, or involved in, money laundering.

Money laundering though not defined in the Act, can be construed to mean directly or indirectly attempting to indulge in any process or activity connected with the proceeds of crime and projecting it as untainted property. The Act stipulates that whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but may extend to seven years and also be liable to a fine which may extend to five lakh rupees.

Money laundering involves a process of getting the money from illegal sources, layering it in any legal source, integrating it as part of any legal system like banking and actually using it. Since the banking as

an industry has a major and significant role to play in the act of money laundering, it is now a serious responsibility on the part of banks to ensure that banking channel is not used in the criminal activity. Much more than a responsibility, it is now a compliance issue as well.

Obligations of banks include maintenance of records of all transactions of the nature and value specified in the rules, furnish information of the transactions within the prescribed time, whenever warranted and verify and maintain records of the identity of all customers. Hence, as a corollary, adherence to Know Your Customer norms and maintenance of all KYC records assumes a very major significance and becomes a compliance issue. Records of cash transactions and suspicious transactions are to be kept and reported as stipulated. Non compliance on any of these will render the concerned bank official liable for the offence of money laundering and guilty under the Act.

e-Records Maintenance Policy of Banks:

Computerisation started in most of the banks in India from end 80's in a small way in the form of stand-alone systems called Advanced Ledger Posting Machines (Separate PC for every counter/activity) which then led to the era of Total Branch Automation or Computerisation in early or mid 90's. TBA or TBC as it was popularly called, marked the beginning of a networked environment on a Local Area Network under a client-server architecture when records used to be maintained in electronic manner in hard-disks and external media like tapes etc for backup purposes.

Ever since passing of the ITA and according of recognition to electronic records, it has become mandatory on the part of banks to maintain proper computerized system for electronic records. Conventionally, all legacy systems in the banks always do have a record maintenance policy often with RBI's and their individual Board approval stipulating the period of preservation for all sorts of records, ledgers, vouchers, register, letters, documents etc.

Thanks to computerisation and introduction of computerized data maintenance and often computer-generated vouchers also, most of the banks became responsive to the computerized environment and quite a few have started the process of formulating their own Electronic Records Maintenance Policy. Indian Banks' Association took the initiative in bringing out a book on Banks' e-Records Maintenance Policy to serve as a model for use and adoption in banks suiting the individual bank's technological set-up. Hence banks should ensure that e-records maintenance policy with details of e-records, their nature, their upkeep, the technological requirements, off-site backup, retrieval systems, access control and access privileges initiatives should be in place, if not already done already.

On the legal compliance side especially after the Rules were passed in April 2011, on the "Reasonable Security Practices and Procedures" as part of ITAA 2008 Section 43A, banks should strive well to prove that they have all the security policies in place like compliance with ISO 27001 standards etc and e-records are maintained. Besides, the certificate to be given as an annexure to e-evidences as stipulated in the BBE Act also emphasizes this point of maintenance of e-records in a proper ensuring proper backup, ensuring against tamperability, always ensuring confidentiality, integrity, availability and Non Repudiation.

This policy should not be confused with the Information Technology Business Continuity and Disaster Recovery Plan or Policy nor the Data Warehousing initiatives. Focus on all these three policies (BC-DRP, DWH and E-records Maintenance Policy) are individually different, serving different purposes, using different technologies and maybe coming under different administrative controls too at the managerial level.

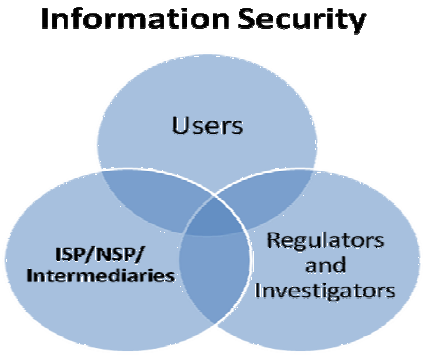
Legislations in other nations:

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber crimes going into all the facets of cyber crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act.

In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled by them. The Sarbanes-Oxley Act (SOX) signed into law in 2002 and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, Children's Online Privacy Protection Act etc.

In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc are all regulatory legislations already existing in the area of information security and cyber crime prevention, besides cyber crime law passed recently in August 2011. Similarly, we have cyber crime legislations and other rules and regulations in other nations.

Conclusion: To sum up, though a crime-free society is Utopian and exists only in dream-land, it should be constant endeavour of rules to keep the crimes lowest. Especially in a society that is dependent more and more on technology, crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DoS or DDoS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of cyber crime and become punishable offences. Hence, it should be the persistent efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.



It should be the duty of the three stake holders viz i) the rulers, regulators, law makers and investigators ii) Internet or Network Service Providers or banks and other intermediaries and

iii) the users to take care of information security playing their respective role within the permitted parameters and ensuring compliance with the law of the land.

Source: Book on "IT" Security of IIBF Published by M/s TaxMann Publishers

****