International Journal of Current Research in Multidisciplinary (IJCRM) *ISSN: 2456-0979*
Vol. 5, No. 5, (May'20), pp. 07-16

CYBER SECURITY-LAW AND STRATEGY: INDIAN & INTERNATIONAL PERSPECTIVE

Dr. Rajeev Kr. Singh
PhD (Cyber Security), Chankya National Law University, Patna, Bihar

ABSTRACT:
Cyber Security is one of the most critical issues the India faces today, and it is also considered to be a hot topic in International level. Mirroring the growth and proliferation of various technologies on the internet, computer network and related cyber crime, cyber law today encompasses several laws and judicial answers to various legal issues. Despite the best intentions of those involved with previous cyber legislative efforts, a regulatory basis simply will not work. It will not improve security and may actually lower it by providing a false level of comfort and tying the private sector down with outdated regulations. Cyberspace's dynamic must be acknowledged and added by polices that are equally dynamic. The present Cyber Security- Law of India is still trying to catch up with cyber criminal and much need to be done in this regard. The IT act deserves a complete restricting as it is creating trouble for law-abiding people and is weak for cyber criminal. At that time there is need of India must learn from International experience especially in the field of confidentiality, privacy and technology in respect of hacking as well as National Security. This paper briefly describes the legal as well as technical security issues especially electronic signature, encryption, interception and monitoring which are by far the biggest concerns regulation and enforcement.

Keyword: *Cyber Security, Cyber Law, Cyber Crime, Data Security Law, Cyber Space, Electronic Signature, Encryption, Interception and Monitoring.*

INTRODUCTION

The security of sensitive data and the system within which they are processed stored is a mission-critical issue for many organizations. As well as being an asset, data can be liability if they are not accorded sufficient protections. In the India they are literally hundreds of government departments, public authorities, educational establishment, healthcare providers, and profit making companies and others that can attest to this fact. Of course, security breaches and data loss are not new phenomena; they are as old as the hills, predating the invention of the computer and the mass adoption of new technologies.

There are series of factors at play here. The number and volume of data processing operations are increasing exponentially year-on-year, which means that the number of security incidents will increase correspondingly. It is essential that some important factors get grip with the process of law reform and advancements in types and form of regulation as well as technologies.

One of the core goals of the data security is ensuring the confidentiality, integrity and availability of data and computer systems. Thus the cyber crime convention groups together the offences of illegal access, illegal interception and monitoring, data interference, system interference and misuse of devices, which is called "offences against the confidentiality, integrity and availability of computer data and system.

The legal recognition of electronic recorded and electronic signature and the methods of authentication of legal records introduced by the Information Technology (IT) Act 2000 ushered in the age of e-filling and e-records in India. Since 2007, all filing with the registrar of companies in

India are made through electronic filings only although paper filings are required also to be made for certain transactions. Since 2008, all income tax returns are filed through e-filings. In India, e-banking has taken early stages with bank statements available to be viewed online.

As the internet is wildly used for activities ranging from browsing to electronic commerce, security mechanism's such as encryption standards assume tremendous important. In the digital age, encryption is essential to protecting the privacy rights of citizens and is views as important tools in maintaining privacy against oppression. Encryption law in India is at a nascent stage. This impression is given by the fact that the IT Act 2000 only contains the cryptic sentence in section 84A that the control Government may prescribe the modes or methods of encryption. But as yet, no policies or guidelines have been issued pursuant to the powers set forth in section 84 A.

In Mumbai, November 26, 2008, terrorist used satellite phone and possibly also Voice Over Internet Protocol (VOIP) to remain in contact. In order to preventing this situation from recurring, by 2009, the IT Act, 2000 had been amended with a view in particular, to prevent terrorists from using electronic communication media to perpetrate their crimes. A central pillar of the law enforcement regime is monitoring, decryption and interception which are vital to gathering the electronic intelligence data necessary to prevent further terrorist attacks. While section 69 of the IT Act, 2000, prior to the amendments, provided the government the right to intercept data amendments, which introduced the new section 69A and 69B, extended this power to interception, monitoring and decryption of data.

Finally, we have facing problem in the area of electronic data communication; challenges of data mishandling; effects of technological change and business process evaluation; rapid growth of electronic commerce likely to pose legal problems as to validity and authenticity of data and information. We have challenges in development of the regulatory regime will need carefully attention, to ensure the India remains a safe country in which to live and work, and essential for developing confidence in the security of electronic transactions.

Finally, in respect of hacking and National Security our major objectives are to understand the technical as well as legal recognition of electronic records and electronic signature, to analyse interception and monitoring of data in cyber space, and to compare the law in developed countries related to electronic communication.

We have already some mechanism to prevent fraud in electronic communication as well as cyber crimes to regarding electronic signature to ensuring the confidentiality, integrity and availability of data; Encryption to protecting the privacy rights of citizens and level of trust in the internet, particularly in e-commerce; and interception and monitoring vital to gathering the electronic intelligence in the interest of public safety.

ABOUT DIGITAL SIGNATURE

A digital signature is an electronic substitute for a manual signature. It serves the same function as a manual signature i.e. primarily that of authentication. In more technical terms, a digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key.

DIGITAL SIGNATURE VS ELECTRONIC SIGNATURE:

The IT Act defines **'Digital Signature'** as "authentication of any electronic record by subscriber by means of an electronic method or procedure in accordance' with the provision of section 3. Section 3, in term; provide that 'any subscriber may authenticate an electronic record by affixing his digital signature'. Further, the authentication of the electronic record must be affected by the use of the

asymmetric crypto system and Hash function which envelop and transform the initial electronic record in to another electronic record.

As per the IT Act 2009 amendments, an '**electronic signature'** is defined as 'authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature. The definition of the 'electronic signature' provide in the 2009 amendments differ from that provided in the UNCITRAL Model Law. This model law based on the "function equivalent approach". This model law also introduced asymmetric cryptography system. The UNCTIRAL Model Law states: 'Electronic Signature' means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

It is important to mention that the electronic techniques to be used for creation of electronic signatures are yet not specified in the IT act and have not yet been specified in the second schedule. Therefore, while the 2009 amendments make electronic signature technologically neutral, as yet, there are no authentication technical specified in the second schedule.

International aspect on Electronic Signature:
There are three types of electronic signature identified by the directive.

- **a.** Electronic Signature
- **b.** Advance Electronic Signature
- **c.** Advanced electronic signature based on a "qualified certificate".

Electronic Signature simply defines as 'data in electronic form which are attached to or logically associated with other electronic data and which serves as a method of authentication'. They do not involve any special security factors, which limits their values for the purpose of data authentication. **Advance Electronic Signature** are defined as electronic signature that are 'uniquely linked to the signatory', 'capable of identifying the signatory', 'created using means that the signatory can mention under his sole control' and one 'linked to the data to which it relates in such a manner that any subsequent changes of the data is detectable'. **Advanced electronic signature based on a "qualified certificate** are generated by 'signature–creation devices'. A signature–creation device is defined as 'configured system or hardware used to implement the signature–creation data'. Signature creation data is defined as 'unique data, such as codes or private cryptography electronic signature'.

Key differences between UNCITRAL Model Law and IT Act in respect of Electronic Signature:

I. The UNCITRAL Model Law specifies other methods, of electronic authentication in addition to asymmetric cryptography. The UNCITRAL Model Law embodies the principle of technological neutrality. In contrast, prior to the 2009 amendments, the IT Act recognised only digital signature and asymmetric cryptography such as Biometric devices based on handwritten signatures, PIN's and digitised versions of handwritten signatures. In these biometric devices, the signatory is to sign manually using a special pen either on a computer screen or on a digital pad. The IT Act was amended in 2009 so as to introduce the concept of electronic signatures which includes but are not limit to digital signatures. However, the new technologies to the used in creation of digital signature are yet to be identified and the second schedule to the IT Act, 2000 remains empty. Moreover, the provisions on digital signatures remain in the text of the IT Act instead of having been relegated to a schedule. This has resulted in the analogous situation in which the IT Act claims to be technology on digital signature and the asymmetric cryptography in the text of the Act.

II. As per the UNCITRAL Model Law, Article 1, that the model law show apply where electronic signature are used in respect of commercial activities like any trade transaction for the supply to exchange of goods or services, distribution agreement commercial representative of agency- factory, leasing, consulting, financing banking, insurance etc. The IT Act contrast, does not state that electronic signature wil be applicable to commercial activities in general. As we know, the IT Act, in the first schedule specifies enumerates the documents of transactions to which the IT Act will not apply. These include negotiable instruments (other than a cheque), a power of Attorney, a Truest Dead, a Will and any contract executed for the sale or conveyance of immovable property or any interest in such property. Therefore, electronic signature cannot be used for the forgoing transaction.

III. The UNCITRAL Model Law holds the certification provider (the intermediary) absolutely responsible in discharging its digital relating to the electronic signatures. The IT Act, on the other hand, does not burden the intermediaries with such absolute liability. Section 79 of the IT Act limits the liability of the intermediaries in certain cases. The intermediary will not be held liable for any third party information, data or communication link if the transmission has not been initiated by him.

The Uniform Electronic Transaction Act (UETA) in respect of Electronic Signature:
The UETA is the uniform law in the US which is intended to remove the barriers to electronic commerce by validating electronic records and signatures. Section of UETA gives legal recognition to electronic records and electronic signatures. The UETA is very flexible in the sense that it recognised all form of electronic signatures and does not restrict the use of ES based on the types of technology used in their creation.

Similarities of UETA, IT Act and UNCITRAL Model Law:
The scope of applicability of electronic signature under UETA is similar to the IT Act 2000, which excludes wills and Trust. Apart from this UETA treats all forms of ES equally, that is, no specific technology need be used in order to create a valid signature. Therefore, the UETA is technology neutral similar to the UNCITRAL Model Law and IT Act 2000 post the 2009 amendments.

Cross Border issues in respect of Electronic Signature
Various difficulties when ES are used in cross border transaction because technical Criteria for validity of ES vary in different jurisdiction. Certain jurisdiction adopt a neutral technology called the "minimalist approach" because its gives the minimum legal recognition to the form of ES whereas some countries adopt a specific technology in creating and authenticating ES. In effect 2009 amendment the IT Act recognised only digital signature created through asymmetric cryptography.

The Future of Electronic Signature:
The current trend in laws and legislative proposal is to link the question of signature validity with certificate of identity. It seems likely that, as commercial activity on the internet increases, business will increasingly require their customers to identify themselves through ID Certificates, and will demand electronic signatures which are validated by those certificates. Use of uncertificated electronic signatures will probably be confined to non commercial transactions; as these will really have legal consequences, the evidential issues of providing signatory identity will be unlikely to trouble the court excessively.

There is also a clear trend towards introducing accreditation schemes for certification authorities, this trend will be supported by the advantages of electronic signature supported by a certificate from an accredited Certification Authority. Such signature will avoid the difficulties inherent in providing of effectiveness of the Signature method in achieving the required evidential functions and will also

benefit from reciprocal recognition in those jurisdictions which make the use of accredited Certification Authorities compulsory as a condition of electronic signature validation.

UNDERSTANDING OF ENCRYPTION

As per the definition 'Encryption' means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality. In the digital age, encryption is essential to protecting the privacy rights of citizens and is viewed as an impotent tool in maintaining privacy against oppression by the state. At the same time, policy makers view encryption as a tool which may be used by criminal to evade surveillance by law enforcement agencies.

Encryption software or hardware uses a mathematical algorithm called cipher to scramble the information in plaintext format to an unreadable format called cipher text. The cipher text can be deciphered only by someone who possesses the de-cryption key. With the use of the de-cryption key, the cipher text is converted back to understandable plaintext.

There are several types of encryption; however, modern computerised encryption uses mainly one type, that is, 'subscription' encryption. In subscription encryption, the message is encrypted by substituting one character for another.

The legal issues raised by the use of encryption are first, whether the commercial use of encryption software and hardware by private individuals and companies should be allowed and, if so, to what level of encryption. Second, whether the private and commercial use of encryption should be subject to the 'key escrow' or otherwise known as; key recovery' requirement, that is, users of encryption must deposit their secret keys with the government or another third party. This is to enable Government agencies. Police to decode the massage without their knowledge. The third issue is to what extent the export of encryption software and hardware should be prohibited if at all. Embedded in these questions is the quintessential conflict between the interests of individuals in privacy and the interest of society in security and law enforcement.

The encryption law in India are at a nascent stage, the IT Act 2000 as amended by the IT (Amendment) Act, 2008, provides for the formulation of a separate encryption policy by the Government and authorises the Central Government to prescribe the modes or methods of encryption. But IT Act , 2000 fails to lay down any general legal principles regarding the commercial use of encryption by individuals of companies and does not specify whether the same is allowed or not.

Encryption Aspect of DoT, TRAI, SEBI and RBI:

Under the Department of Telecommunication (DoT) regulation encryption can be freely used only up to the obsolete 40 bit level. Current encryption technology cannot be used by an ISP without prior approval from the DoT and deposit of the De-cryption key. Therefore, any encrypted mail or other messaging service provided by an Indian ISP will necessarily be subject to escrow and the Government can interrupt private messages at any time.

The Telecom Regulatory Authority of India (TRAI) has also made recommendations regarding encryption standard in the context of value added service. TRAI has recommended the registration of value added service providers (VASP) with the DoT as other service Providers (OSP). In this regard, the TARI has recommended that the VASP registered as OSP be prevented from the employment of bulk encryption equipment in the provision of VAS. Moreover, if encryption equipment higher than the 40 bit key length in the symmetric key algorithm or its equivalent in other algorithm or as prescribed by DoT, from time to time, are to be deployed, then the VASP must obtain prior written permission of the access service providers and deposit the de-cryption key, split into two parts, with the access service providers or DoT.

I addition to the DoT and the TRAI, the securities Exchange Board of Indian (SEBI) has also prescribe guidelines relating to encryption. A committee constituted by SEBI, recommends that advance security products used for e-commerce may be made optional, including 64 bit/128 bit encryption.

There is a contradiction between the view taken by the DOT/TRAI and SEBI. The DoT allows the free use of encryption only up to 40 bits and requires a written permission for use of encryption with a higher bit level along with deposit of the decryption key. In contrast, the committee constituted by SEBI advocates use of advance security products, including 64 bit. 128 bit encryption.

After That Reserve Bank of India (RBI) has stipulated certain technological and security standard that, (a) all mobile banking shall be permitted only by validation through a two factor authentication. (b) One of the factors of authentication shall be mPIN or any higher standards. (c) Where mPIN is used, end to end encryption of the mPIN shall be ensured, i.e mPIN shall be stored in a secure environment.

International Perspective of Encryption:

***US laws on Encryption*:** After the terrorist attacks on September 11, 2001, the US Government proposed wider surveillance power wherein the Government officials and law enforcement agencies would be empowered to have a back door access to encryption products. In other word, the law enforcement agencies should have a master key for all strong computer encryption algorithms in order to check and curb terrorist activities, in the interest of national security. The law enforcement authorises sought not only access to encrypted messages but also to columnisations as they occur in 'real time.'

In the U.S, several encryption standards have been developed, in particular, the data Encryption Standards (DES), the Escrowed Encryption Standards (EES) and the Advanced Encryption Standards (AES).

The **DES** is a cryptography algorithm which uses 56-bit binary keys for encrypting and decrypting binary coded information. Here encrypting data converts it to an unintelligible form called cipher. Decrypting Cipher converts the data back to its original form called plaintext. Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorised recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data.

DES subsequently became considered to be insecure for many applications because the 56- bit key size is too small and the DES became vulnerable to brute force attacks. In addition, the DES was designed primarily for hardware and is relatively slow when implemented in software; DES has been withdrawn as a standard by the National Institute of Standards and Technology.
The requirement for the new standards is that a block size of 128 bits has to be specified and key sizes of 128, 192 and 256 had to be supported. The cipher had to be secure and speed was also considered important. It also had to be capable of running in extremely small embedded systems within limited amounts of RAM and ROM.

EES is a standard for encrypted communications that was approves by the US Department of Commerce in 1994 and is better known by the name of an implementation called the Clipper Chip. The Clipper Chip is an encryption device to enable the Government to de-crypt and intercept a phone call encrypted with a clipper phone and then put the essential information into 'escrow".

The Encryption/de-cryption algorithm used by EES is called SKIPJACK. This algorithm can be incorporated into communications devices including voice, facsimile (Fax) and computer data. In other words, use of cipher device would have resulted in every telephone, fax, modem or other communications equipment manufactured or sold in India being subject to de-cryption and interception by the US Government authorities.

AES announced by National Institute of standard and Technology after a 5 years standardization process in which fifteen competing design were evaluated. The AES is a symmetric –key encryption standards developed by two Belgian cryptographers. Each of These Ciphers has 128 bit block size, with key sizes of 128, 192 and 256 bits, respectively.

i. ***UK laws on Encryption*:** there have historically been no domestic use restriction nor any import controls on encryption products in the US. The UK has been a major supporter of the attempt made by the US to require key escrow. Under the regulation of Investigatory Power Act (RIPA) 2000, the UK government is allowed access to encryption keys or decryption data with effect from October 1, 2007. Under an order issued under section 49, part III of RIPA, the police or intelligence agency staff can be made legally liable for breaches of the security of seized cryptography keys or the protected material disclosed. In April 1998, the UK department of Trade and Industry (DTI) published the 'secure electronic commerce statement' in April 1998 which sought to promote security in e-commence through encryption. On January 28, 1998, the DTI authorised an 'open General Export License' for personal computers accompanying their users that contain encryption. On-line voice encryption/decryption programmes are not covered by the special permit.

ii. ***Legal Position in France:*** France has historically prohibited the right to use encryption hardware and software. However, in 1997, there was a move to liberalize this position with the intention of promoting the penetration of French companies into the e-commerce market that had been dominated by US Company's since the inception. The French Government also raised the threshold for permitted encryption methods from 40 bit to 128 bits, a level recommended by experts to ensure high security. The regulations concerning the supply of encryption products was sought to be simplified. Moreover, the laws relating to the constraints imposed on the third parties was sought to be liberalised through appropriate measures.

iii. ***Legal Position in Germany:*** Germany has always been in favour of liberal use of Encryption. Germany law did not restrict the import of encryption or the use of encryption software or hardware. The German Government has extended its support of the OECD guidelines on cryptography. Germany has, however, also support US efforts to promote key escrow. On June 11, 1997, Germany enacted a digital Signature Law (SigG). The Digital Signature system necessitated the use of asymmetric encryption. The encryption algorithm to be used was, however, not defined by law. This system required a secret key to be held by the signer and a public key that is certified by a Certificate Authority which has procured a license from the Government communications authority.

iv. ***Legal Position in China:*** China is one of the most challenging enjoinments for cryptography use and regulation. Import and export of encryption products require a license from the state Encryption Management Commission. This also applies for foreign individuals and firms operating in China, who must report details of their encryption system to, and receive approval to use those products form National commission on encryption code regulation (NCECR).

MONITOR AND INTERCEPTION

Monitoring and interception has long been permissible with respect to telephony. Section 5 (2) of the Indian Telegraph Act of 1985 provides that, on the occurrence of a public emergency or in the interest of public safety the Government has the Right to intercept any communications made through telephone services provided the permission has been obtained from the Union Home Secretary or Principal Secretary Home. Reportedly, over 6000 telephones in New Delhi have been tapped.

On October 27, 2009, the Ministry of communication and IT notified rules under section 69, 69A and 69B setting forth the procedures for interception , monitoring and decryption of data, collection of traffic data and blocking of access to website.

At present under rule 419 (A), the state and central agencies at present can tap phones for 7 days in stretch without permission. This period has been reduced to 72 hours. The tradition methods of intercepting data and bloking website are at router level and on the basis of IP address. However, this is a crude method as an entire website must be blocked because of a small part of its contents.
Deep Packet Inspection (DPI) is a sophisticated method refers to the interception of online data from emails, intent phone calls, as well as image and messages on social networking sites such as facebook and twitter. DPI reportedly used by many Canada's ISP to monitor which application is generating more data traffic or which type of data particular customers use. Nevertheless, DPI has raised privacy concern in both the US and Canada with people protecting over the fact that a network operator could track each website a user surfed, record the details of every search and read every mail. While DPI was used by Canadian ISPs for improving their billing to customers, DPI has also been used by Govt. for Political Purposes.

In fact, the 2009 amendments to the IT act were controversial in that the poser to monitor and intercept information and block websites are traditionally associated with non-democratic societies and are inimical to right to free speech associated with democratic India. However not only China and Iran but also democratic society such as the US and Europe also engage in monitoring and interception of Information. One of the earliest developed systems for monitoring and interception of data is the **Carnivore Software** platform in the US.

The use of Carnivore software did result in public protest in the US. As a result of the negative publicity, the FBI changed the name of the system form Carnivore to DCS 1000 which stands for 'Digital Collection system.' In 2005, the FBI replaced Carnivore with an improved commercially available software known as Narusinsight. In addition to monitoring and interception of data, another power of the State against cyber crime is the blocking of website.

As per Section 69 of the Information Technology Act, 2000, an officer specially authorised by the Central Government or a State Government may order any Government agency to not only intercept, but also monitor of decrypt any information transmitted. In addition to adding the power for monitoring and decryption, the 2009 Amendments also added new sections 69A and 69B. The section 69A empowers the central government to direct any agency or intermediary such as an ISP to block access to websites. The New section 69B, in turn, empowers the Central Government to Authorised any agency to monitor and collect traffic data or other information transmitted through any computer resource.

Monitoring and Interception under US Law:
Section 202 of the US Patriot Act (P.L. 107-56) allows the US Government to intercept wire, oral and electronic commendation relating to computer fraud and abuse offences. Under Section 212 of the Patriot Act, ISPs and network administrators may give law enforcement agencies access to their networks without a warrant in order to track criminal activities. Section 217 allows a person acting

under colour of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances. Under section 216 of the Patriot Act, a single court order authorizing the use of a pen Register or trap and trace device can be used to apply those devices to nay computer or facility anywhere in the country. One of the earliest developed system for monitoring and intercepting of data is the Carnivore Software (DCS 1000) platform in US.

Monitoring and Interception in the UK:

The regulation of Investigating Powers Act (RIPA) confers the British Government with the power , subject to obtaining an interception warrant, to access 'communications data', including internet traffic data for the purpose of national security, detecting or preventing crime, preventing disorder, in the interest of the UK's economic well being, in the interest of public safety of protecting public health. RIPA allows the British government to access and gather information regarding email communication, a person's uses of the interest and creates a profile of the target person and his internet usage.

The European commission had taken the position that UK has failed to comply with EU rules protecting the confidentially of electronic communications such as email or surfing the internet, which are protected under the privacy Directive and the data protection Directive and the EC even commenced an infringement processing against UK. According to the European commission, there are three main gaps in the UK rules governing the confidentiality of electronic communications:

- **a.** There is no independent national authority to supervise interception of communications, although the establishment of such authority is required under the ePrivacy and data protection Directives, in particular, to hear complaints regarding the interception of communications.
- **b.** The Regulation of 2000, RIPA authorised the intercept of communications not only where the persons concerned have consented to intercept but also when the person intercepting the communications are 'reasonable grounds for believing' that consent to do has been give. These UK law provisos do not comply with EU rules defining consent as freely given specific and informed indication of a person's wishes.
- **c.** The RIPA provisions prohibiting and providing sanctions in case of unlawful interception are limited to 'intentional' interception only, whereas the EU law required member states to prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.

The above comparative analysis show that both the patriot Act in the US and the Regulation of Investigatory Powers Act in the UK differ significantly from India's IT act and the Rule there under. The former require Government officials to obtain a court order engaging in the monitoring, interception and decryption of data and the same can be done without a court order only upon obtaining the consent of the concerned individuals. In contrast, the ultimate authority in the Indian legal regime is a bureaucrat, either the Ministry of Home Affairs at the central level or the Secretary, Home Department at the state level.

Finally, on the basis of study, govt. of USA, UK, France, Germany law enforcement agencies in all these countries are similar problems. Although, the degree of the lost lawful interception currently caused by the use of encryption in different countries is variable. These countries with these this issue desire to co-operate with other Govt. to tackle the impact of encryption on law enforcement.

CONCLUSION & SUGGESTION

a. An interesting side-effect of the challenge posed by electronic Signatures is that the question of whether a seal can function as a signature becomes relevant. The reason for this is that many of the electronic signature technologies require the signatory to use a numerical key to produce the signature. The smallest

useful key area minimum of 56 bit in length, offering a range of numbers between approximately 563,000,000,000,000 and 72,000,000,000,000,000 in decimal notation. These key are too small for adequate security, however, and 128 bit or large r key are more desirable. Number of this size is not easily memorable or easily keyed in without error, and so the key are normally stored on some physical device, such as a memory stick or a smart card.

b. The recent Amendments to the IT Act, 2000, nearly a decade after the Act came into force; promise to take electronic commerce to the next level by making introducing the concept of technological neutrality. Since electronic signatures are no longer necessarily based on asymmetric cryptology, technical advancement can easily be implemented. These technological advances are most likely to make electronic signature easier and more secure to use.

c. In the matter of encryption, all over an interesting question is whether the presence of encryption renders the underlying information confidential. As a starting point it would seen that if a person goes to the length of encrypting information the information must have a quality about it that is deserving of protection. However there is no authority in law that holds that the mere presence of encryption renders the underlying information confidential.

d. In the case of Mars UK Ltd. Vs Teknowledge Ltd., which concerned a coin discriminator mechanism for the sorting of coins in coin operated machines, the defendant reserved engineered the mechanism, a process that required the decryption of encryption programme code. One was the question before the court was whether the presence of encryption put the defendant on notice that the encrypted information was confidential.

e. In the matter of Interception , Decryption and monitoring, one of the controversial provisions that has been engrafted into the I.T Act, 2000 by the amendments through the I.T (Amendment) Act, 2008, is the substitution of section 69 that in its new *avatar* grants certain authorities also the power of interception, decryption and monitoring electronic contents including communications (e-mail, online chat or mobile phone communication) " for investigation of any offence" under the sun as against the traditional powers that wee highly restricted on few grounds such as, in the interest of the sovereignty or integrity of India.

f. The amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Govt. may prescribe the modes or methods of encryption. As yet no polices or guidelines have been issued pursuant to the power set forth in section 84A.

g. The IT Act 2008 allows the central government to intercept computer communication for investigation of any offence. Section 26 of the Indian Post office Act 1898 grants the government the power to intercept letter or postal articles on the happening of any public emergency or in the interest of public safety or tranquillity. Section 5 (2) of the Indian Telegraph Act, 1885 empower the government to intercept land line and mobile phones on the occurrence of any public emergency , in the in the interest of public safety , Sovereignty and integrity of India, security of state, friendly relation with foreign states, public order, or for preventing incitement of the commission of an offence. However the IT amendment Act enlarges of the poser of the central government to embrace interception of information transmitted through any computer resource for the purpose of investigation of any offence. The provision is also vague about the procedure and safeguards that need to be employed when such interception or monitoring or decryption is carried out.

h. The standing committee on information technology , while reviewing the bill , observed that 'public order' and 'police ' are state subjects as per schedule VII of the Constitutions and that the IT Bill should confer powers of interception on the stat governments also in tune with the provisions of section 5(2) of the Indian Telegraph Act, 1885. Therefore interception of information should be for the perception of certain cognizable offence in addition to the already prescribes grounds, instead of the broad sweeping term of 'the commission of any cognisable offence or for investment of any office' used in the Act.

i. The Amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Government it further does not define the procedure and safeguard subject to with blocking access by public to any information through any computer resource may be carried out.

j. Lack of harmonized definition of the cyber crimes and lack of international cooperation in tacking the menace is the other problems which require immediate solution.