IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers

By

Karnika Seth*

Abstract

In the year 2000, India enacted its first law on Information Technology namely, the Information Technology Act,2000. The IT Act,2000 is based on the Model law of E-commerce adopted by UNCITRAL in 1996. The preamble to the IT Act, 2000 points out a three fold objective , firstly, to provide legal recognition for transactions carried out through electronic means, secondly, to facilitate the electronic filing of documents with government agencies, and thirdly to amend certain Acts, interalia, the Indian Penal Code,1860, Indian Evidence Act, 1872. The IT Act, 2000 gave legal validity and recognition to electronic documents and digital signatures and enabled conclusion of legally valid & enforceable e-contracts. It also provided a regulatory regime to supervise the Certifying Authorities issuing digital signature certificates and created civil and criminal liabilities for contravention of the provisions of the IT Act,2000. It also conferred on the Central Government the power to appoint Adjudicating Authority to adjudge whether a person has committed a contravention within the meaning of the Act and conferred on this Authority the powers vested in a civil court. With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act,2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act,2000.

This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act,2008 has brought marked changes in the IT Act,2000 on several counts.

*Karnika Seth is a practicing cyberlawyer & Managing Partner of Seth Associates, a Law firm based in India. She is the Chairperson of the Cyberlaws Consulting Centre and the Author of the book titled "Cyberlaws in the Information Technology Age" published in 2009 by Butterworths lexisnexis that discusses the evolution of Cyberlaws across different jurisdictions including India, USA, U.K and Europe.

In this Paper I intend to discuss the major changes brought about by the IT (Amendment) Act ,2008 & comment on its effectiveness in the context of Indian cyberlaw. I have also suggested few strategies to meet with the intended objectives of the amended Act for an overall effective implementation.

There are also challenges posed by the amended Act that can be foreseen and our country needs to be well equipped to overcome these challenges. Further, there are still some lacunae in the amended Act which I have briefly discussed at appropriate places. The role of Adjudicating Authority in the amended Act is very significant. The subject matter of its jurisdiction, adjudging matters alleging contravention and awarding compensation under chapter 9 is explained in clearer terms in the Amended IT Act . The amended Act also curtails the power & jurisdiction of the Adjudicating officers and excludes those matters where compensation claimed is more than 5 crores. This paper discusses the important dimensions that emerge from the recent amendments and challenges that will be faced by the Adjudicating officers in complying with its prescribed duties under the IT Act,2008.

At the outset, I would like to express my gratitude to the Hon'ble Members of the National Project Committee on Enforcement of Cyberlaw for giving me the opportunity to present this paper in the National Seminar on Enforcement of Cyberlaw at New Delhi on 8 May 2010. I hope this paper will fulfill the intended purpose.

IT ACT, 2000 vs IT (Amendment) Act, 2008

(1**) Electronic signatures introduced**-

With the passage of the IT (Amendment) Act,2008 India has become technologically neutral due to 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. This is a positive change as India has different segments people and all may not be technologically adept to understand and use the digital signatures . Therefore, allowing

forms of authentication that are simpler to use such as retina scanning can be quite useful in effective implementation of the Act. However, the challenge it poses is accessibility to authentication tools and imparting education to people to use the same . It is a challenging task for the Central government to prescribe conditions for considering reliability of electronic signatures or electronic authentication techniques under Section 3A (2), the procedure for ascertaining electronic signature or authentication under Section 3A(3),the manner in which information may be authenticated by electronic signatures in Section 5. It also involves expenditure as such authentication tools will require purchase, installation & training, particularly in all government departments where it is proposed to be used. Equally challenging will be the drafting of duties of subscriber of electronic signature certificate under Section 40 A of the Act which will need to incorporate security measures subscribers can adopt depending on electronic signature being used for signatures. Further, in a move to secure the flow of data and information on the internet, and promote e-commerce & e-governance, the amended Act in Section 84A has empowered the Central Government to prescribe modes or methods for encryption. These parameters should be laid down in consultation with organizations such as Nasscom and/or governmental agencies that can assist in formulation of necessary standards and related rules.

(2) **Corporate responsibility introduced in S. 43A**

The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of *'reasonable security practices'* to maintain its secrecy, failing which they may be liable to pay damages. Also, there is no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the IT Act,2000 whereby all persons responsible to the company for conduct of its business shall be held guilty incase offence was committed by a company unless no knowledge or due diligence to prevent the contravention is proved.

Insertion of this provision is particular significance to BPO companies that handle such sensitive information in the regular course of their business. This provision is important to secure sensitive data and is hence a step in the right direction. However, the challenge is to

first elucidate what we qualify as " *reasonable security practices*" . The Act in explanation to Section 43A indicates these procedures designed to protect such information from 'unauthorised access, damage, use, modification, disclosure, or impairment, as may be specified in an agreement between parties' or as may be specified by any law for the time being in force and in absence of both, as may be prescribed by Central Government in consultation with professional bodies/associations. The law explaining the definition of 'reasonable security practices' is yet to be laid down and/or Central government is yet to frame its rules thereon. Perhaps, we can take guidance from certain foreign laws on data protection & standards laid down in European Union or by organizations such as OECD in protection of sensitive personal data. It is a challenge for the Central Government to prescribe in consultation with professional bodies the information that will fall within the meaning of "sensitive personal data or information". To describe what these parameters should be is beyond the scope of this Article but is an interesting issue for discussion.

(3) Critique on amended section 43 of IT Act-

The amended Act provides the distinction between '*contravention*' and '*offence*' by introduction of the element of mens rea for an offence (s 43 for contraventions and s 66 of the Act for offences). It is pertinent to note that no ceiling limit for compensation is prescribed under s 43 of the Amendment Act, 2008 which was one crore rupees in the IT Act. The removal of the ceiling limit can be misused or abused particularly seen in instances where company files frivolous claims against its ex-employee who may have joined a competitor firm without breaching its employment contract.

In my opinion, one major diversion from the earlier IT Act is the fact that the amended Section 43 has the insertion of Section 43 (i) & (j)in the amended Act which may require an element of mens rea with actus reus. Particularly Section 43(j) requires presence of *mens rea (please note use of words 'stealing' and 'intention to cause damage'* in the section*)* and the same acts mentioned in section 43 when committed 'dishonestly' or 'fraudulently' are punishable under amended Section 66. The intent behind this change is to not only punish the offender for its criminal act but also to compensate the victim with pecuniary damages for loss incurred

due to acts of the offender. In my view this is a positive change since a ceiling on compensation that may be awarded in s. 43 renders at risk those companies that invest huge amounts of money in their research & development and an employee simply steals way that valuable information or resource by electronic means without due remedy or award of compensable damages.

The relevant provision is as under-

> " *If any person without the permission of the owner or any other person who is incharge of a computer , computer system or network…. Steal, causes,destroys or alters or causes any person to* ***steal,*** *conceal,destroy or alter any computer source code used for a computer resource* ***with an intention to cause damage****… he shall be liable to pay damages by way of compensation to the person so affected* ."

The intention of the amended Act is to introduce the element of intention in this clause of the Section and this mens rea element also finds its roots in Section 66 where a person will be sentenced if he does the same act 'dishonestly' or 'fraudulently' within the meaning of IPC i.e with intention to defraud or cause wrongful loss. 'Intention to cause damage' in S.43(j) can be said to also include intention to cause wrongful loss. Per se '*stealing*' cannot be done without the mens rea in place and therefore this act should fall under s.66 and not 43 incase S.43 is to cover only acts done inadvertently or by negligence. This certainly cannot be the intention /objective of the amendment. Hence, a clarification on this point is necessary.

(4) Important definitions added

Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(ha)- "*Communication device* " and Section 2 (w) –"*intermediary*". Although cell phones and other devices used to communicate would fall under the definition of computer in the IT Act.This amendment removes any ambiguity and brings within the ambit of the Act all communication devices, cellphones, ipods or other devices used to communicate, send or transmit any text ,video ,audio or image. The insertion of

definition of 'intermediary' similarly clarifies the categories of service providers that come within its definition that includes telecom service providers,network service providers,internet service provider, webhosting service providers,search engines,online payment sites,online auction sites,online market places and cyber cafes.

(5) **Legal validity of electronic documents re-emphasized**-

Two new sections Section 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents. Section 7A in the amended Act makes audit of electronic documents also necessary wherever paper based documents are required to be audited by law. Section 10A confers legal validity & enforceability on contracts formed through electronic means. These provisions are inserted to clarify and strengthen the legal principle in Section 4 of the IT Act,2000 that electronic documents are atpar with electronic documents and e-contracts are legally recognized and acceptable in law. This will facilitate growth of e-commerce activity on the internet and build netizen's confidence.

(6) Critique on Power of Controller under the amended Act-

Section 28 of the Act provides that the Controller or any authorized officer shall investigate '*any contravention of the provisions of this Act, rules or regulations made thereunder*'

.These words should be replaced with words '*any contravention of the provisions of this Chapter*' in light of the fact that the amendment in Section 29 for Controllers power to access computers and data has been curtailed by removal of words " any contravention of the provisions of this Act, rules or regulations made thereunder" for insertion of words " *any contravention of the provisions of this Chapter*" . Also, the Controller's power cannot mean to overlap with Adjudicating officers who are authorized to adjudicate on cases of contravention that fall under Section 43 or the subject matter jurisdiction of CAT or the Police. Therefore , the power of Controller has to be interpreted keeping in view the intent & objectives of the Act which can be clarified.

The role of the Controller to act as **repository of digital signatures** has been repealed by the IT Amendment Act, 2008. This role has now been assigned to the Certifying Authority in Section 30 of the IT Act. This change poses a major challenge to ensuring the secrecy and privacy of electronic signatures is maintained. The Certifying authorities will bear greater responsibility and need to strengthen their security infrastructure to ensure its role as repository is delivered with efficacy. It will need to allocate more resources and manpower to regularly publish information regarding its practices, electronic signatures certificates and publish the current status of each certificate.

(7) The Role of Adjudicating officers under the amended Act-

The Adjudicating officer 's power under the amended Act in Section 46 (1A) is limited to decide claims where claim for injury or damage does not exceed 5 crores. Beyond 5 crore the jurisdiction shall now vest with competent court. This has introduced another forum for adjudication of cyber contraventions. The words 'competent court' also needs to be clearly defined. As per Section 46(2),the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers.This leaves a wide room for subjectivity and quantum should be decided as far as possible objectively keeping in view the parameters of amount of unfair advantage gained amount of loss caused to a person (wherever quantifiable), and repetitive nature of default. The Information Technology (qualification and experience of adjudicating officers and manner of holding enquiry) Rules,2003 lay down the scope and manner of holding inquiry including reliance on documentary and other evidence gathered in investigations. The rules also provide for compounding of contraventions and describe factors that determine quantum of compensation or penalty.

In the IT Act,2000 the office of adjudicating officer had the powers of civil court and all proceedings before it are deemed to be judicial proceedings. A new change is incorporated in Section 46(5)© whereby the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment of receiver. This empowers the office of Adjudicating officer and extends greater enforceability and effectiveness of its orders.

(8) **Composition of CAT-**

The amended Act has changed the composition of the Cyber Appellate Tribunal .The Presiding officer alone would earlier constitute the Cyber Regulations Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. The qualifications for their appointment, term of office salary , power of superintendence, resignation and removal, filling of vacancies have been incorporated. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority.

It is pertinent to note that there has not been any amendment in Section 55 by 2008 amendments which states that no order of CAT shall be challenged on ground that there existed a defect in constitution of appellate tribunal. However, in my view this runs contrary to principles of natural justice. An analogy is drawn to Arbitrations where defect in constitution of a tribunal renders an award subject to challenge as per Indian laws.

(9) New cybercrimes as offences under amended Act-

Many cybercrimes for which no express provisions existed in the IT Act,2000 now stand included by the IT (Amendment) Act, 2008. Sending of offensive or false messages (s 66A), receiving stolen computer resource (s 66B), identity theft (s 66C), cheating by personation (s 66D), violation of privacy (s 66E). A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment that may extend to imprisonment for life . Section 66 F covers any act committed with intent to threaten unity ,integrity,security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency , morality, or in relation to contempt of court, defamation or incitement to an offence , or to advantage of any foreign nation, group of individuals or otherwise. For other offences mentioned in Section 66 , punishment prescribed is generally upto three

years and fine of one/two lakhs has been prescribed and these offences are cognisable and bailable. This will not prove to play a deterrent factor for cyber criminals. Further, as per new S. 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new S. 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence.

In certain offences, such as hacking (s 66) punishment is enhanced from 3 years of imprisonment and fine of 2 lakhs to fine of 5 lakhs. In S. 67, for publishing of obscene information imprisonment term has been reduced from five years to three years (and five years for subsequent offence instead of earlier ten years) and fine has been increased from one lakh to five lakhs (rupees ten lakhs on subsequent conviction). Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extend to 5 years with fine upto ten lakhs. This provision was essential to curb MMS attacks and video vouyerism. Section 67B punishes offence of child pornography, child's sexually explicit act or conduct with imprisonment on first conviction for a term upto 5 years and fine upto 10 lakhs.This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.
Punishment for disclosure of information in breach of lawful contract under sec 72 is increased from 2 yrs upto 5 yrs and from one lakh to 5 lakh or both.This will deter the commission of such crime. By virtue off Section 84 B person who abets a cybercrime will be punished with punishment provided for that offence under the Act. This provision will play a deterrent role and prevent commission of conspiracy linked cybercrimes. Also, punishment for attempt to commit offences is given under Section 84 c which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both.

10) **Section 67 C to play a significant role in cyber crime prosecution-**

Section 67 C brings a very significant change in the IT Act,2000 .According to this section, intermediaries shall be bound to preserve and retain such information as may be prescribed by the Central government and for such duration and format as it may

prescribe. Any intermediary that contravenes this provision intentionally or knowingly shall be liable on conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lac or both.

Many cybercrime cases cannot be solved due to lack of evidence and in many cases this is due to the fact that ISP failed to preserve the record pertaining to relevant time .This provision is very helpful in collection of evidence that can prove indispensable in cybercrime cases.

11) Section 69- Power of the controller to intercept amended

Section 69 that deals with power of Controller to intercept information being transmitted through a computer resource when necessary in national interest is amended by Section 69.In fact the power vests now with the Central Government or State Government that empowers it to appoint for reasons in writing, any agency to intercept, monitor or decrypt any information generated , transmitted , received or stored in any computer resource . This power is to be exercised under great caution and only when it is satisfied that it is necessary or expedient to do so in interests 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 . The procedure and safeguards to exercise this power are laid out by the Information Technology (procedure and safeguards for interception , monitoring and decryption of Information) Rules, 2009 . The subscriber or intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 7 yrs and imposition of fine. The element of fine did not exist in the erstwhile Section 69. The said rules provide ample safeguards to ensure the power in this section is diligently exercised, with due authorization procedures complied with and not abused by any agency/intermediary including maintaining confidentiality and rules for maintaining or destruction of such records.

12) **Power to block unlawful websites should be exercised with caution-**

Section 69A has been inserted in the IT Act by the amendments in 2008 and gives power to Central government or any authorized officer to direct any agency or intermediary(for reasons recorded in writing) to block websites in special circumstances as applicable in Section 69.Under this Section the grounds on which such blocking is possible are quite wide. In this respect, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 were passed vide GSR 781(E) dated 27 Oct 2009 whereby websites promoting hate content, slander, defamation,promoting gambling,racism,violence and terrorism, pornography, violent sex can reasonably be blocked. The rules also allow the blocking of websites by a court order.It further provides for review committee to review the decision to block websites. The intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 7 yrs and imposition of fine. We need to use this power with caution as it has a thin line that distinguishes reasonable exercise of power fro Censorship.

13) **Section 69B added to confer Power to collect, monitor traffic data**

As a result of the amendments in 2008 , Section 69 B confers on the Central government power to appoint any agency to monitor and collect traffic data or information generated ,transmitted, received,or stored in any computer resource in order to enhance its cybersecurity and for identification,analysis, and prevention of intrusion or spread of computer contaminant in the country . The Information Technology (procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009 have been laid down to monitor and collect the traffic data or information for cyber security purposes under Section 69B .It places responsibility to maintain confidentiality on intermediaries, provides for prohibition of monitoring or collection of data without authorization. This prescribes stringent permissions required to exercise the powers under this Section which are fully justified as abuse of this power can infreinge the right to privacy of netizens. It also provides for review of its decisions and destruction of records. The intermediary that fails to extend cooperation in this respect is punishable offence with a term which may extend to 3 yrs and imposition of fine.

14) **Significance of the term "Critical Information Infrastructure "**

Section 70 has a very important definition added by the IT (amendment) Act,2008. The explanation to Section 70 defines what is "critical information infrastructure" .It encompasses the computer resource the destruction of which not only has an adverse impact on defence of India but also economy, public health or safety. This is very significant step as today our IT infrastructure may also be used to manage certain services offered to public at large, destruction of which may directly affect public health and safety . Hence, their protection is equally important as is the maintaining of security and sovereignty of India.

By virtue of Section 70 A and B Indian CERT has been appointed as the National nodal agency for critical information infrastructure protection. The CERT shall play an indispensable role in maintaining cybersecuriy within the country. A very important step is coordination between CERT and service providers, data centres, body corporates,and other persons (Section 70B (6)). That will lead to effective performance of the role of CERT in. It has multiple roles education ,alert system , emergency response, issuing guidelines , reporting of cyberincident amongst other functions . Incase any person fails to comply with its directions, such person shall be punishable with imprisonment of term that may extend to one year and fine of one lakh or both. It also excludes the court from taking cognizance of any offence under this section except on a complaint made by authorized officer of CERT to prevent misuse of the Section.

15) **Important clarifications on the Act's application & effect**

By virtue of Section 77 in the amended Act, it has been clarified that awarding of compensation ,penalty imposed or confiscation made under this Act shall not prevent the award of compensation,or imposition of any other penalty or punishment under any law for the time being in force.This Section can be read with Section 81 proviso wherein it is clarified that IT Act shall not restrict any person from exercising any right conferred under copyright Act, 1957 or patents Act, 1970.

16) **The combined effect of Section 77 and 77 B-**

By virtue of Section 77 Compounding of offences other than offences for which imprisonment for life or punishment for a term exceeding has been provided has been made possible. Section 77 B makes offences punishable with imprisonment of three years and above as cognizable and offence punishable with 3 years of punishment as bailable. Since the majority of cyber crime offences defined under the amended IT Act are punishable with imprisonment for three years, the net effect of all amendments is that a majority of these cybercrimes are bailable. This means that the moment a cybercriminal is arrested by the police, barring a few offences, in almost all other cyber crimes, he has to be released on bail as a matter of right, by the police. A cyber criminal, once released on bail, will immediately attempt at destroying or deleting all electronic traces and trails of his having committed any cyber crime. This makes the task of law enforcement agencies extremely challenging.

17) Combined effect of Section 78 & 80-

The Section 78 of the Act is amended to confer power to investigate offences under the Act from DSP level to Inspector level. This will be instrumental in quicker investigation in the cybercrime cases provided adequate tools and training is provided.

Section 80 has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of inspector or any authorized officer of central government or state government. Such officer is empowered to arrest without warrant a person found therein who is reasonably suspected of having committed or of committing or being about to commit any offence under this Act. However, this section may be misused easily. Unless it is reasonably suspected that a person has committed , is committing or is about to commit an offence, he should not be arrested without warrant . Otherwise cybercafés , in particular could be adversely affected.

18) Liability of Intermediary amended-

The earlier section 79 made network service providers liable for third party content only when it fails to prove that the offence was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention. The burden of proof was on the network service provider. The amended Section 79 states that the intermediary shall not be liable for any third party information if it is only providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted or the intermediary does not initite the transmission, select the receiver and select or modify the information contained in transmission. It provides that the Intermediary shall be liable if he has conspired or abetted or induced,whether by threats or promise or otherwise in the commission of the unlawful act (Section 79(3)(a). However, it is pertinent to note that the onus to prove conspiracy has now shifted on the complainant. This may be extremely difficult for a complainant to prove.

Section 3 (b) renders an intermediary liable in case upon receiving actual knowledge or on receiving notice from a government agency, the intermediary fails to expeditiously remove or disable access to the unlawful material without vitiating the evidence in any manner.

19) Examiner of Electronic Evidence created-

With amendments in 2008, Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence. This agency will play a crucial role in providing expert opinion on electronic form of evidence The explanation to the Section has an inclusive definition of "*electronic form evidence*" that means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence,digital audio, digital video,cellphones , digital fax machines.With the increasing number of cybercrime cases it will become necessary to set up atleast one Examiner of Electronic Evidence in each State. The CFSIL laboratory in Hyderabad is playing similar role at present in cybercrime

cases where forensic study of hard discs and other computer accessories, digital equipment is undertaken to provide expert opinion on the digital evidence analysed.

Conclusion

The IT(Amendment) Act,2008 from an overall perspective has introduced remarkable provisions and amendments that will facilitate the effective enforcement of cyberlaw in India. India is now technologically neutral with electronic signatures replacing the requirement of digital signatures . The importance of data protection in today's information technology age cannot be undermined and it finds place in Section 43,43A, ,66, 72 of the IT Act,2000. In this era of convergence the definition of 'communication device' and 'intermediary' have been rightly inserted/revisited and validity of e-contracts is reinforced by insertion of Section 10 A. . Section 46(5)© of the IT Act is a welcome provision that empowers the Adjudicating officers by conferring powers of execution on the office of Adjudicating officer at par with a civil court.Plethora of new cybercrimes have been incorporated under chapter XI as offences under the amended Act to combat growing kinds of cybercrimes particularly, serious crimes such as child pornography, and cyber terrorism.The Intermediaries have been placed under an obligation to maintain and provide access to sensitive information to appropriate agencies to assist in solving cybercrime cases under Section 67C, Section 69. However, liability of ISPs has been revisited and onus shall lie on complainant to prove lack of due diligence or presence of actual knowledge by intermediary as proving conspiracy would be difficult. These are some of the challenges that cyberlaw enforcement teams will be faced with The power of interception of traffic data and communications over internet will need to be exercised in strict compliance of rules framed under respective Sections in the Act conferring such powers of monitoring, collection , decryption or interception. Power for blocking websites should also be exercised carefully and should not transgress into areas that amounts to unreasonable censorship. Many of the offences added to the Act are cognizable but bailable which increases the likelihood of tampering of evidence by cybercriminal once he is released on bail. The police must therefore play a vigilant role to collect and preserve evidence in a timely manner .For this , the police force will need to be

well equipped with forensic knowledge and trained in cyberlaws to effectively investigate cybercrime cases.The introduction of Examiner of Electronic Evidence will also aid in effective analysis of digital evidence & cybercrime prosecution.

Having discussed the new amendments and challenges before Indian cyberlaw regime , employing the strategies recommended below can facilitate the enforcement of cyberlaws in our country –

(1) educating the common man and informing them about their rights and obligations in Cyberspace. The practical reality is that most people are ignorant of the laws of the cyberspace, different kinds of cybercrimes, and forums for redressal of their grievances. There is an imperative need to impart the required legal and technical training to our law enforcement officials, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyberlaws .

(2) The reporting and access points in police department require immediate attention. In domestic territory, every local police station should have a cybercrime cell that can effectively investigate cybercrime cases . Accessibility is one of the greatest impediments in delivery of speedy justice.

(3) Also we have only one Government recognized forensic laboratory in India at Hyderabad which prepares forensic reports in cybercrime cases. We need more such labs to efficiently handle the increasing volume of cybercrime investigation cases. Trained and well-equipped law enforcement personnel - at local, state, and global levels can ensure proper collection of evidence, proper investigation, mutual cooperation and prosecution of cybercases.

(4) Further under Section 79 of the IT Act ,2000 no guidelines exist for ISPs to mandatorily store and preserve logs for a reasonable period to assist in tracing IP addresses in Cybercrime cases. This needs urgent attention and prompt action.

(5) The investigation of cybercrimes and prosecution of cybercriminals and execution of court orders requires efficient international cooperation regime and procedures. Although Section 1(2) read with Section 75 of the IT Act,2000, India assumes prescriptive jurisdiction to try accused for offences committed by any person of any nationality outside India that involves a computer, computer system or network located in India, on the enforcement front, without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition.

IT (Amendment) Act, 2008 is a step in the right direction , however, there are still certain lacunae in the Act, (few of which were briefly pointed out in this paper) which will surface while the amendments are tested on the anvil of time and advancing technologies!

****