CHAPTER – VII
CONCLUSION AND SUGGESTIONS

CONCLUSION

The revolution brought by the Internet and the World Wide Web is having an immense impact on all aspects of human existence. Cyber crime is the fastest growing crime in the world with millions of people affected every day. With the invention of computers, its increasing use and human dependency over Internet, while we have gained mainfolds in terms of efficiency and management, it has also brought to the front many negative effects and disadvantages. Traditional concepts of criminal liability are inadequate and different from the mode of culpability in cyber crimes. Cybercrime continue to grow and focus on the business sector, enterprises realize that they must adopt a security strategy that protects their network systems and data from malicious content arriving via the web, as well as preventing data leakage in outbound web traffic.

The problems associated with cyber crimes are not limited to formulating substantive criminal laws. The unique characteristics of these types of crime make even the traditional procedural laws archaic. Also these problems are not restricted to prosecution of cyber crimes alone but extend to many other fields of criminal investigation. For example, the very criminal law enforcement systems in many of the nations are not equipped with the kind of skills that are necessary in investigating a cybercrime.

The traditional rules of investigation and evidence collection are often no sufficient in the investigation of cybercrimes. Coupled with this is the transnational nature of the crime. The criminal activity could be initiated in one country by accessing a system in another country and still the result could be felt in many other countries. Also the speed, absence of distance and borders, sophistication etc of the cyberspace further complicates the investigation and prevention of cybercrimes.
Cyber crimes is emerging as a serious threats. The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their 'virtual' counterparts. Effective law enforcement is complicated by the transnational nature of cyber space. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Such techniques dramatically increase both the technical and legal complexities of investigating and persecuting cyber crimes.

A cyber crime knows no geographical boundary; the absence of international cooperation between police forces adds to the woes of victims and lets the culprit go scot free.

Cyber crime is one such kind of crime where different societies are likely to rule differently. As a result what may be a crime within the jurisdiction of one country may not be so in the jurisdiction of another. This would, very obviously, create unique problems in the enforcement of law. Since electronic crimes can simultaneously be committed across borders, questions of national sovereignty are also the important issues to be taken into consideration. Today's computer network's have removed barrier for the cyber criminals. Police officials, investigators, prosecutors and judges alike are struggling hard to catch up with the emerging situations. In some cases, countries are requesting for the extradition of computer hackers who have never even physically entered the country whose they have allegedly broken. Law enforcement officials are contending with new computer-based evidence that must convince a court of the authenticity and show that it has not been electronically altered. Internet communications, as a matter of fact, can easily be routed through many different jurisdictions, thus making tracing of the cyber rogues indeed very difficult. Electronic evidence or proceeds from electronic transactions can easily be moved to locations where a lack of effective laws or technical expertise puts them beyond the legal recourse. Data can be encrypted to make it difficult for law enforcement agencies to read. The spread of networks in the developing world is proceeding at slower pace. Many developing countries are caught in between the need to go 'on line' to spur economic development and the desire to prevent cyber crime. The lack of a legal framework
creates greater opportunities for offenders to commit economic crimes beyond their home countries.

Cyber crime has emerged as a major source of headache for governments across the world. The absence of any international law on cyber crime further complicated matters with different countries assuming distinct national approaches for controlling, regulating and preventing cyber crime.

The International Cyber Crime Treaty promises to become the first international benchmark for controlling and regulating cyber crime and for ensure cooperation among different signatory nations for exchanging information concerning cyber crime and cyber criminals. The International Cyber Crime Treaty is yet to come into implementation. However, almost single handedly the treaty to fill up the void about the need for having an international regulatory mechanism for controlling cyber crime that has existed since the beginning of internet.

The International Cyber Crime Treaty also becomes the first international treaty to be in place for any issue concerning cyber laws. The treaty may not be perfect, and no treaty is perfect. However, it does not give a very wrong starting point for international efforts to regulate and control cyber crime.

Whereas the benefits of electronic revolution have reached in each and every nation of the world, most nations do not, however, have got separate domestic law to deal with the problem of cyber crimes. Nor are there any mutual agreements and multilateral treaties between the nations. Nor, at least to the best of knowledge of the present authors, there is any such international agreement/convention/ declaration/ protocol/ resolution/to deal with cross-border cyber crimes. The absence all these have made countries vulnerable to the threats of cyber crimes. Therefore, there is no denying the fact that an international agreement on the ways and means of dealing with cyber crime is urgently required to address the problem in a holistic manner.

Capacity of human mind is unfathomable. It is possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the
witness that no legislation has succeeded in totally eliminating crime from the
globe. The only possible step is to make people aware of their rights and duties (to
report crime as a collective duty towards the society) and further making the
application of the laws more stringent to check crime.

Indian Parliament has adopted two fold strategies to control cyber crimes.
It has amended Indian Penal Code to cover cyber crimes expressly and has
provided provision in the Information technology Act, 2000. This has basically
enacted to facilitate e-commerce in India, to deal with computer related crime.
The I.T. Act, 2000 was undoubtedly a welcome step at a time when there was no
legislation on this specialized field. The I.T. Act, 2000 is a comprehensive
legislation, but contains many lacunae. The IT Amendment Bill 2008 has been
passed by the Lok Sabha and the Rajya Sabha on 23rd Dec., 2008. Subsequently
the IT (Amendment) Act, 2008 received the assent of President on 5th Feb. 2009
and was notified in Gazette on 27 Oct., 2009.1

The cyber law, in any country of the world, cannot be effective unless the
concerned legal system has the following three pre requisites:-

1. **A Sound Cyber Law Regime:** The Cyber Law in India can be found in
the form of IT Act, 2000. Now the IT Act, as originally enacted, was
suffering from various loopholes and lacunae. These “grey areas” were
excusable since India introduced the law recently and every law needs
some time to mature and grow. It was understood that over a period of time
it will grow and further amendments will be passed to make it compatible
with the International standards. It is important to realize that we need
“qualitative law” and not “quantitative laws”. In other words, one single
Act can fulfill the need of the hour provided we give it a “dedicated and
futuristic treatment”. The dedicated law essentially requires a consideration
of “public interest” as against interest of few influential segments. Further,
the futuristic aspect requires an additional exercise and pain of deciding the
trend that may be faced in future. This exercise is not needed while
legislating for traditional laws but the nature of cyber space is such that we

---

1 See Appendix-I
have to take additional precautions. Since the Internet is boundary less, any person sitting in an alien territory can do havoc with the computer system of India. For instance, the Information Technology is much more advanced in other countries. If India does not shed its traditional core that it will be vulnerable to numerous cyber threats in the future. The need of the hour is not only to consider the “contemporary standards” of the countries having developed Information Technology standards but to “anticipate” future threats as well in advance. Thus, a “futuristic aspect’ of the current law has to be considered. Now the big question in whether India is following this approach? Unfortunately, the answer is in NEGATIVE. Firstly, the IT Act was deficient in certain aspects, though that was bound to happen. However, instead to bringing the suitable amendments, the IT Act, 2000 amendments have further “diluted” the criminal provisions of the Act. The “national interest” was ignored for the sake of “commercial expediencies”. The amendments have made the IT Act a “tiger without teeth” and a “remedy worst than malady”.

(2) A Sound Enforcement Machinery:- A law might have been properly enacted and may be theoretically effective too but it is useless unless enforced in its true letter and spirit. The law enforcement machinery in India is not well equipped to deal with cyber law offences and contraventions. They must be trained appropriately and should be provided with suitable technological support.

(3) A Sound Judicial System:- A sound judicial system is the backbone for preserving the law and order in a society. It is commonly misunderstood that it is the “sole” responsibility of the “Bench” alone to maintain law and order. That is a misleading notion and the “Bar” is equally responsible for maintaining it. This essentially means a rigorous training of the members of both the Bar and the Bench. The fact is that the cyber law is in its infancy stage in India hence not much Judges and Lawyers are aware of it. Thus, a sound cyber law training of the Judges and Lawyers is the need of the hour.
Establishment of E-Courts in India is an aspect of Judicial and legal reforms in India. Till June 2010, we are still waiting for the establishment of first e-court in India. India does not have even a single e-courts and the proposed e-courts project has failed miserably in India despite all government claims.

The various loopholes in the IT (Amendment) Act, 2008 are as follows:-

The IT (Amendment) Bill, 2008 was passed in an unprecedented hurry, without any discussion in both the houses of the parliament in the last week of Dec. 2008.

The issues relating to confidential information and data of corporate and their adequate protection have not been adequately addressed. The said law is not a comprehensive law on data protection or on digital secrets. Having a couple of sections on data protection does not serve the requirements of corporate India.

India has neither learnt from the wisdom of the United States nor the European Union, in terms of their respective experiences, in the area of data protection. The amended provisions will not aid the victim entities, whose data and information is often misused by their employees or agents with impunity.

The IT Act Amendments are also deficient in the sense that they do not create rebuttable presumptions of confidentiality of trade-secrets and information, in the contest of corporate India. A large number of Indian companies and individuals are saving their confidential data, information and trade-secrets in the electronic form on their computers. Given the apparent increase in technology adoption, it is increasingly being found that that despite all precautions been taken, the employees are still going ahead and taking away confidential data from companies. The inability of the law to create enabling presumptions of confidentiality regarding corporate and individual data and information in the electronic form, is likely to complicate matters further for Indian companies and netizens.

Given the move to take an extremely lenient view on most cybercrimes, corporates need to forget about being able to get their errant employees, misusing their confidential data and information, behind bars. Absence of an effective
remedy for corporates by the new amendments is likely to further erode the confidence of the Industry in the new cyber legal regime. The maximum damages by way of compensation stipulated by the new cyber law amendments are Rs 5 crore. When calculated in US Dollar terms, this is a small figure and hardly provides any effective relief to corporates, whose confidential information worth crores is stolen or misused by its employees or agents.

Another major failure of the proposed amendments is that they have not dealt with the entire issue pertaining to Spam, in a comprehensive manner. In case, the word Spam is not even mentioned anywhere in the IT Amendment Act. India has missed yet another opportunity to deal with the contentious issue of Spam.

It is pertinent to note that the countries like USA, Australia and New Zealand have demonstrated their intentions to fight against Spam by coming across with dedicated anti-spam legislations. However, in India, we neither have any anti-Spam legislation, nor we have any specific provisions for effective prevention and regulation of Spam. This make India a heaven as far as, Spam is concerned. This is all the more serious since India already features in the top ten nations of the world from where Spam originates.

Any major failure of the IT Act Amendments is that they have not specifically detailed with the issues pertaining to electronic discovery. Today, increasingly people and entities as also corporate are relying upon electronic evidence and electronic media as a means of communicating with each other and doing business. However, the Indian IT Act Amendments are completely silent on the issues of electronic discovery. This once again shows the short sightedness of the Indian IT Amendments Act to address the complicated emerging issues pertaining to electronic discovery.

The IT Act amendments do not address jurisdictional issues. At a time when the Internet has made geography history, it was expected that the new amendments would throw far more clarity on complicated issues pertaining to jurisdiction. This is because numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to
assume enabling jurisdiction over data and information impacting India, in a more comprehensive way than in the manner as sketchily provided under the current law.

The new amendments make it mandatory for corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices, and procedures”. However, what would be these “reasonable security practices and procedures” would be anybody’s guess. It has to be pointed out that one set of security practices will not fit the entire nation. What would be reasonable security practices for one industry may not be directly applicable to another industry. No maintaining such reasonable security practices would expose the said corporate to civil liability to pay damages by way of compensation to the person so affected, to the tune of Rs 5 crore. The new amendments are likely to impact all industries, which use computers, computer systems and computer networks and data and information in the electronic form. These reasonable security practices and their mandatory adoption, while in overall better interests, are likely to unveil a package of unpleasant surprises for many.

The most startling aspect of the new amendments is that these amendments seek to make the Indian Cyber law 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 that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; 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.

A perusal of the said legislation shows that there is hardly any logical or rational reason for adopting such an approach.
Currently, the IT Act 2000 has provided for punishment for various cyber offences ranging from three years to ten years. These are non-bailable offences where the accused is not entitled to bail as a matter of right.

However what amazes the lay reader is that the amendments to the IT Act have gone ahead and reduced the quantum of punishment. Taking a classical case of the offence of online obscenity, Section 67 has reduced the quantum of punishment on first conviction for publishing, transmitting or causing to be published any information in the electronic form, which is lascivious, from the existing five years to three years. Similarly, the quantum of punishment for the offence of failure to comply with the directions of the Controller of Certifying Authorities is reduced from three years to two years.

Further, it is shocking to find that the offences of hacking, as defined under Section 66 of the existing Information Technology Act 2000 has been completely deleted from the law book. In fact, the existing language of the under Section 66 has now been substituted by new language. Deleting hacking as a specific defined offence does not appeal to any logic. The cutting of certain elements of the offence of hacking under the existing Section 66 and putting the same under Section 43 make no legal or pragmatic sense. This is all the more so as no person would normally diminish the value and utility of any information residing in a computer resource or affect the same injuriously by any means, with the permission of the owner or any such person who is in charge of the computer, computer system or computer network.

At that time when the entire world is going hammer and tongs against Cyber Crimes and Cyber Criminals, here comes a contrary trend from the Indian legislature. Cyber criminals of the world targeting India or operating in India need not despair. The legislation has now stipulated that Cyber crimes punishable with imprisonment of three years shall be bailable offences. Since the majority of cyber crime offences defined under the amended IT Act are punishable with three years, the net effect of all amendments is that a majority of these cybercrimes shall be bailable. In common language, this means that the moment a cybercriminal will be
arrested by the police, barring a few offences, in almost all other cyber crimes, he shall be released on bail as a matter of right, by the police, there and then.

Keeping in account human behavior and psychology, it will be but natural to expect that the concerned cyber criminal, once released on bail, will immediately go and evaporate, destroy or delete all electronic traces and trails of his having committed any cyber crime, thus making the job of law enforcement agencies to have cyber crime convictions, a near impossibility.

The fertile liberal treatment meted out to cyber criminals, by the new IT Act amendments, facilitating the environment where they can tamper with, destroy and delete electronic evidence, is likely to make a mockery of the process of law and would put the law enforcement agencies under extreme pressure, apart from exposing corporate to undesirable headaches. In the 14 odd years since internet have been commercially introduced in our country, India has got only three cyber crime convictions. This has made India a safe haven for cyber criminals and cyber crimes are increasing in India at a speed that India cannot control.

Another major change that the new amendments have done is that cyber crimes in India shall now be investigated not by a Deputy Superintendent of Police, as under the existing law, but shall now be done by a low level police inspector. So, henceforth, the local police inspector is going to be the next point of contact, the moment a person or any company is a victim of any cyber crime. The efficacy of such an approach is hardly likely to withstand the test of time, given the current non-exposure and lack of training of Inspector level police officers to cyber crimes, their detection, investigation and prosecution.

Given this new development, it is probable that the concept of e-hafta or electronic hafta is likely to be far more reinforced and developed as an institutional practice. This is so as the law has now produced more powers to the inspector than ever before, regarding cybercrimes.

The expectations of the nation for effectively tackling cyber crime and stringently punishing cyber criminals have all been let down by the extremely liberal amendments, given their soft corner and indulgence for cyber criminals.
The entire issue relating to Encryption as a process, has not been satisfactorily dealt with. Having a single provision in the new amendments, reserving the right to specify processes relating to encryption later, does not do justice to the expectations of corporate India, regarding the usage of encryption.

Encryption is a process that scrambles information, such that it cannot easily be understood by people who do not have the right key to unscramble it. The level of security this provides depends critically on the length of the keys used in the encryption and decryption process. The maximum permissible length of this key has been a matter of debate, discussion and dispute between the technology industry and the government. The implications of this are highly significant for commerce, law, intellectual property protection, and civil liberties.

Rather than addressing the complicated issues of encryption and defining a comprehensive policy on encryption, the new amendments have merely decided to defer the said issue and leave it to the route of secondary legislation by means of rules and regulations. This makes the situation all the more complicated, given the existing position.

India's Guidelines and General Information for Setting up of International Gateways for Internet and similar documents stipulate that "encryption upto 40-bit key length in the RSA algorithms or its equivalent in other algorithms can be used without having to obtain permission. If encryption equipments higher than this limit are to be deployed, it needs permission of the Telecom Authority and deposit the decryption key, split into two parts, with the Telecom Authority."

The practical problem is that encryption upto 40 bits of length is absurdly easy to crack, even by schoolboys. Today, banks and financial institutions are openly violating the official limit of 40 bit encryption. At a time, when the world is moving towards one direction, India should not be seen to be moving in the opposite direction.

India needs to harness the benefits and advantages of technology, rather than wanting to ride its boat upstream, against the current of the technological river.
The IT Act Amendments, 2008 are likely to adversely impact corporate India and all users of computers, computer systems and computer networks, as also data and information in the electronic form.

Other users of the Social Networking Websites (SNWs) could be made defending parties to the defamation suit, whether or not they were aware of such defamatory statements. However, the new amendment will provides a certain line of defence to them provided they satisfy the above mentioned conditions set out under the new section 79.

The IT (Amendment) Act, 2008 does not deal with cyber squatting cyber defamation, online intellectual property rights, cyber espionage, theft of trade secrets etc.

Section 69 of the IT (Amendment) Act, 2008 appears to be in violation of Article 21 of the Constitution-"no person shall be deprived of his life or personal liberty except according to procedure established by law". It is unfortunate that a democratic and independent India has passed a law which is fear more detrimental to personal liberty than the British Raj did.

Online Education and E-Learning in India: Online education in India received two fatal blows this year. Firstly there was a failure of the online examination conducted by IGNOU and then India witnessed the collapse of Common Admission Test (CAT) exams. This shows that India is still not ready for online education and e-learning in India. Even the legal framework for the same is also not conducive and is counterproductive.

Unique Identification Project of India: India adopted Unique Identification Project and constituted Unique Identification Authority of India (UIAI) this year. However, the same is not legitimate in the absence of proper legal framework in this regard that is presently missing. The project also fails to meet the requirements of "Human Rights Protection in Cyberspace".

Serious Frauds and White Collar Crimes: Serious Frauds and White Collar Crimes are increasing in India at a rapid speed. Now the criminals are using
ICT to further their acts for committing these crimes. In the absence of stringent laws in this regard, India is becoming a favorite destination for these crimes.

**Crime Reporting by Media:** The Delhi High Court has constituted a committee to formulate guidelines for crime reporting by the media. The GOI also constituted a task force for the Broadcasting Authority of India. The choice between self regulation or government enacted laws is still not clear. There is an emergent need of broadcasting laws and regulations in India.

**Internet Banking Frauds:** Internet Banking frauds are increasing in India at an alarming rate. With a weak cyber law, lack of cyber security awareness and increasing e-surveillance initiatives in India, Internet banking disputes are bound to increase in India. The government is least bothered about these issues and ultimately the account holders would have to bear the financial losses.

**E-Surveillance in India:** With the passage of IT Act 2008 India has now officially become an endemic e-surveillance society. The amendments have provided unregulated, unconstitutional and arbitrary e-surveillance powers to GOI and its agencies and instrumentalities. The fact is that India has become an E-Police State without any regard to "Human Right Protection in Cyberspace". Confidential information is already vulnerable and with the proposed Indian plans of installing key loggers at cyber cafes, the same would exclude the use of cyber cafes for these purposes. Although cyber cafes are not a good place to transact confidential matters yet with a poor Internet penetration in India this may still happen.

**Indian E-Governance Failures:** There are many factors that ail e-governance of India and make it highly unsuccessful in the Indian context. The net result is that National E-Governance Projects like E-Bharat have died due to absence of proper management, transparency and accountability. Now with the World Bank taking the management of the E-Bharat in its own hands we may expect the revival of the same.

**Lack of awareness**—One important reason that the Act of 2000, 2008 is not achieving complete success is the lack of awareness among the people about their rights. Further most of the cases are going unreported.
Unfortunately, the I.T. (Amendment) Act, 2008 was cleared by Indian government despite these warnings and India has now become a hub for cyber criminals. These limitations and weaknesses of the cyber law amendment led to a death of the exclusive cyber law of India.

In spite of some drawbacks in the Information Technology Act, the future of cyber law in India is very bright. India is leading developing country and it will maintain its leading in future also. It has taken drastic info-tech steps and has been successful in focusing the attention of the White House. In the year 2000, the White House sent a message that former U.S. President Mr. Bill Clinton would like to visit Indian Cyber Savvy at his best. Though the city of Bangalore is more established cyber center yet he visited the City of Hyderabad, which is evolving as a high tech city under the dynamic leadership of Chandra Babu Naidu, Chief Minister of the State of Andhra Pradesh. The visit of Clinton is memorable one.

In the present study an attempt has been made to develop a ‘cyber jurisprudence’ having in view various cyber regulations made in India, U.S.A., U.K., Malaysia, Singapore, Germany, Japan to check the cyber crime and the criminal. During the course of study it has been found that neither the technology nor the legal regulations alone can be helpful to control the cyber crime; rather a combined effort of both is needed.

**SUGGESTIONS**

In the light of discussions made in preceding chapter's and on the basis of conclusion arrived at there from it may humbly be submitted that:-

1. **Public Awareness:** Most people are not aware of extent to which computer crime can affect their lives, finances, and business, family and how fast this menace is growing. Educating the common man and informing them about their rights and obligations in cyber space. Schools and colleges must educate all students about cyber crime. The practical reality is that people are ignorant of the laws of the cyber space, different kinds of cyber crimes, and forums for redressal of their grievances.
(2) **Training of Law Enforcing Agencies:** There is an imperative need to impart the required legal and technical training to our law enforcement officials, including judiciary and the police officials to combat the cyber crimes and to effectively enforce cyber laws.

(3) **E-Courts In India:** The judicial reforms have finally received the attention of the Government of India. However, the quality of Judicial services in India cannot be improved till we have E-Courts in India. Till the end of June 2010 India does not have even a single E-Court despite contrary media reports and rumors. Further, it is also an emergent need of e-courts training of judges and lawyers in India. The establishment of E-Courts in India requires certain pre requisites. These are:-

i) **E-Courts Policy:** Setting Policy for various aspects of E-Courts is the first and foremost requirement. In the absence of a well defined and pre decided framework, no direction can be given to the E-Courts scheme of India.

ii) **Connectivity:** Creating an interconnected system across all court levels is an important aspect of E-courts. The District Courts in India must be connected with High Courts and Supreme Court for better, timely and effective disposal of cases.

iii) **Simplicity And User Friendly:** E-Court mechanism must be not only simple but also be user friendly. The litigants must find the e-Courts facilities in India very easy to adopt.

iv) **Scope:** In India we consider mere computerization as establishment of E-Courts. In reality, E-Courts is much broader than mere computerization and filing facilities.

v) **Authentication:** Authentication plays an important role in fixing attribution and legal responsibility. There must be a “Technology Neutral Mechanism” to authenticate various stages of E-Courts usages.
vi) **Integrity:** E-Courts must ensure integration among court and justice systems.

vii) **Security:** Security of E-Courts Infrastructure and System is of paramount importance. A system must be put in place that provides secure access to case information for appropriate parties.

viii) **Data Keeping:** All the information regarding use of E-Courts facilities must be duly recorded and stored. These include maintaining proper records of e-file minute entries, notification/service, summons, warrants, bail orders, etc for ready and subsequent references.

ix) **Payment Gateway:** A secure, efficient and fully operational payment gateway must be established so that various payments and fees regarding court cases can be made online.

x) **Absence Of Monopoly:** The E-Courts Project must not be given to a single vendor. Instead the E-Court Committee of India must adopt a multiple vendor approach.

(4) **Cyber Crime Cell** - In India we have need to establish Special Cyber Crime Investigation Cell to investigate with well-equipped technology such as firewall, filter software.

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

(5) **Establish Forensic Laboratory** - 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 cyber crime 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 cyber cases.

(6) Further under section 79 of the IT (Amendment) Act, 2008 no guidelines exists for ISPs to store mandatorily and preserve logs for a reasonable period to assist in tracing IP addresses in cybercrime cases. This needs urgent attention and prompt action.

(7) Cyber Pornography: We need more teeth to the law to cope up with the situation. We need to adopt specific and clear definition of cyber crime, cyber pornography, and child pornography in cyber space.

There is great need to impose more responsibilities on the Internet Service Providers and cyber cafes. They must use filter system, firewall software, regular virus scanning system and verify all detail identifications of users i.e. with photo, address, date and time of use of particular computer by particular user and the like. More so, ISPs must have filter process and firewall to prevent cyber pornography.

Cyber cafe owners must take initiatives by monitoring whether any one especially young person is viewing pornographic websites so that they can be prevented and controlled. Cyber cafes must help police by providing every facility they require to control this crime.

Parents can prevent this crime by monitoring their children whether they are spending more time in net during night or when alone. If so whether it was pornographic materials they were looking for? Whether they are receiving e-mails, calls, gifts from unknown person? Whether they have changed the scene frequently? Whether they are not attentive in family affairs? They may require counseling by psychologists.

Computer at home must be kept in common place. Parents must prevent receiving objectionable materials by using firewall, filter software and other tools which are available from time to time.

(8) Cyber Terrorism: The IT Act 2008 has enacted a single provision for meeting the menace of cyber terrorism in India. Although this is a good
step in the right direction yet the government of India (GOI) needs to enact a separate and comprehensive legislation in this regard as a single provision would not prove sufficient in the long run.

(9) **Cyber Security Of Defense Forces:** The defense forces of India also need cyber security and cyber forensics capabilities. The digital life is an altogether different segment where traditional methods are ineffective. The cyber war and cyber terrorism threats are not only real but also very dangerous. India must upgrade its cyber security and national security capabilities as soon as possible. Repeated cyber security breaches have been reported in India from time to time but the attitude of Indian government has not yet changed.

(10) **Hesitation to report offences:** As stated above the of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. For complete realization of the provisions of this Act a cooperative police is require.

(11) The investigation of cyber crimes and prosecution of cyber criminals and execution of court orders requires efficient international co-operation regime and procedures.

(12) A global incident response organization would be the most effective way to facilitate response and to ensure that the process of information exchange is secure, effective, reliable and rapid. Information exchange and interaction between various entities are necessary to produce comprehensive approach and practical solutions to the complex problems. We need to consider the issues that must be addressed to support a global incident response effort and to reduce the likelihood, number and extent of computer security incidents. The global infrastructure for incident response may be implemented through the following structure:-

(i) **International Co-ordination Centre:** We share the responsibility to improve the internet security and co-ordinate effective international global response to computer security incidents and events. To be successful, we must ensure participation and co-
operation among governments, law enforcement agencies, commercial organizations, the research community, and practitioner who have experience in responding to computer security incidents. Establishment of an International coordination centre to provide global response to computer security incidents serves as a multi-level hierarchy with the global centre at the top level and the national infrastructure at the lower level. To be successful, such an international centre must gain constituency, global recognition and trust of every nation in the world.

(ii) Regional Co-ordination Centre: Establishment of a number of suitably located Regional Co-ordination Centre's around the world may co-ordinate response to computer security incidents around the globe. Each of these centre's would act as peers to co-ordinate their efforts, but would be operated separately.

(iii) National Co-ordination Centre's: Establishment of the cyber crime teams for co-coordinating the cyber crime investigation in the territories that fall within the national boundaries is continuing to increase. National boundaries provide a demarcation for policies, procedures, and jurisdiction for information exchange and hence they provide an excellent co-ordination of the cyber crime investigation in various states at the national level. Although these centre's are meant to co-ordinate the efforts put in by the states, it might also undertake an operational incident-handling role, depending on the size of the nation involved.

(13) Establish a National Centre for Computer Crime Complaints, on the pattern of one at the USA. Its key functions should be to receive on-line complaints, analyze them to identify the trends in internet crimes and refer the potential criminal schemes to the Central/State law enforcement agencies. This centre should follow the single-window concept for indentifying the criminal schemes for appropriate enforcement. It can also provide the forensic investigative and analytical support to all the law enforcement and regulatory agencies on a nation wide basis.
Globally Co-ordinate Cyber Laws:- Merely passing national legislation and putting them in force cannot regulate the internet-related activities; it needs a strong political will to push the matter. There is an immediate need of a detailed legal structure followed by institutional arrangements for compulsory jurisdiction of judicial forum to adjudicate such violations. During May 2000, a three-day Cyber Crime Conference was held at Paris. In this Conference, the Interior Minister of France proposed for instituting globally coordinated laws and initiatives to throttle hackers, virus makers, software pirates and other crooks that are making the life of the internet users miserable. A comprehensive international convention, with focus on cyber crimes, should urgently be formulated and an 'International Criminals Tribunal' with global jurisdiction to investigate, try and punish cyber offenders is to be set up.

I.T. (Amendment) Act, 2008 is a step in the right direction, however, there are still certain lacunae in the Act, which will surface while the amendments are tested on the anvil of time and advancing technologies. With growing dynamics of technology in India, the legal matrix needs to be fortified at every milestone to fill up lacunae the remain in information technology laws. India will call for more efficacious and stricter regime for legal enforcement cyber laws. It would be a good idea to seek advice of Techno-Legal Experts this time before formulating the I.T. (Amendment) Act.