CHAPTER SEVEN

CONCLUSIONS AND SUGGESTIONS

CONCLUSION

Looking from an overall perspective, the Information Technology Act, 2000 is a laudable effort by the Government to create the necessary legal infrastructure for promotion and growth of electronic commerce. Prior to the coming into effect of the IT Act, 2000, the judiciary in India was reluctant to accept electronic records and communications as evidence. Even e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. The IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward.

From the perspective of the corporate sector, the IT Act 2000 and its provisions contain the following positive aspects:

The implications of these provisions for the corporate sector are that email is now be a valid and legal form of communication in our country, which can be duly produced and proved in a court of law. The corporates today thrive on email, not only as the form of communication with entities outside the company but also as an indispensable tool for intra company communication. It has been seen that the corporates, in their intra company communications
on email, have not been very careful in using the language of such emails. Corporates ought to understand that they shall need to be more careful while writing emails, whether outside the company or within, as emails, in whatever language, could be proved as a legal document in a court of law, sometimes to the detriment of the company. Even intra company notes and memos, till now used only for official purposes, shall come within the ambit of the IT Act, 2000 and will be admissible as evidence in a court of law. A lot would of course depend upon how these emails are proved in a court of law. A possible consequence of the same for a typical wired company would be that any employee, unhappy with a particular email communication, whether received in a official or personal capacity, may make the email as the foundation for launching a litigation in a court of law. Further, when a company executive sends an email to another executive in the company with some defamatory or other related materials and copies the same to others, there are possibilities that he may land in litigation in a court of law.

Companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian Cyberlaw, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
Corporates will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the IT Act, 2000.

The IT Act, 2000 also throws open the doors for the entry of corporates in the business of being Certifying Authorities for issuing Digital Signature Certificates. The law does not make any distinction between any legal entity for being appointed as a Certifying Authority so long as the norms stipulated by the IT Act, 2000, rules and regulations made thereunder have been followed.

The Act also enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in the electronic form as may be prescribed by the appropriate Government. India is rapidly moving ahead in the field of electronic governance and it will not be long before governments start taking online applications for issuing licences, permits, sanctions or approvals by whatever name called. This provision shall be a great leveler as it will enable all kinds of companies to do much interaction with different government departments online, thereby saving costs, time and wastage of precious manpower.
Corporates are mandated by different laws of the country to keep and retain valuable and corporate information. The IT Act, 2000 enables companies legally to retain the information in the electronic form, if-

a. the information contained therein remains accessible so as to be usable for a subsequent reference;

b. the electronic record is retained in the format in which it was originally generated, sent or received or in a format, which can be demonstrated to represent accurately the information originally generated, sent or received;

c. the details, which will facilitate the identification of the origin, destination, date and time of ends receipt of such electronic record, are available in the electronic record:

The IT Act, 2000 addresses important issues of security, which are so critical to the success of electronic transactions. The Act has given legal definition to the concept of secure digital signatures, which would be required to have been passed through a system of a security procedure, as agreed to by the parties concerned. In
times to come, secure digital signatures shall play a major role in the New Economy, particularly from the perspective of the corporate sector, as they will enable more secure transactions online.

In today's scenario, information is supreme. Information is stored by the companies on their respective computer systems, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by way of compensation, not exceeding Rs.1, 00,00,000.

Corporates in India can now heave a sigh of relief as the IT Act, 2000 has defined various cyber crimes and has declared them penal offences punishable with imprisonment and fine. These include hacking and damage to computer source code. Often, corporates face hacking into their systems. Prior to the coming into effect of the Indian Cyberlaw, the corporates were helpless as there was no legal redress for such issues. But the IT Act, 2000 changes the scene altogether.
However, despite the overwhelmingly positive features of the IT Act, 2000, there are numerous grey areas in the Indian Cyberlaw, which call for amendments in the Indian Cyberlaw:

The Indian Cyberlaw came a bit late. With the phenomenal growth of Internet, which doubles approximately every 100 days, the IT Act, 2000 should have been passed long ago.

The IT Act, 2000 purports to be applicable to not only the whole of India but also to any offence or contravention thereunder committed outside India by any person. This provision in Section 1 (2) is not clearly drafted. It is not clear as to how and in what particular manner, the Act shall apply to any offence or contravention thereunder committed outside India by any person. The enforcement of this aspect of the IT Act, 2000 is an area of grave concern. Numerous difficulties are likely to arise in the enforcement of the IT Act, 2000 as the medium of Internet has shrunk the size of the world, made geography history and slowly, national boundaries shall cease to have much meaning in cyberspace.

It is also strange that Section 1 (4) of the Act excludes numerous things from the applicability of the IT Act, 2000. The IT Act, 2000 does not apply to

i. A negotiable instrument as defined it) Section 13 of the Negotiable Instruments Act, 1881.
ii. a power of attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;

iii. a trust as defined in Section 3 of the Indian Trusts Act, 1882;

iv. a will as defined in clause (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

v. any contract for the sale or conveyance of immovable property or any interest in such property.

There is no logic in excluding negotiable instruments from the applicability of the IT Act, 2000. The net effect of this exclusion is that any dispute regarding payments, received by means of any negotiable instruments for an e-commerce transaction, are excluded from the protection of the IT Act, 2000. In addition, the Indian Cyberlaw does not legalize electronic fund transfer in the country. The IT Act, 2000 already excludes numerous important things. It refers to promoting electronic commerce and begins by excluding immovable property from the ambit of electronic commerce, a reasoning that defies logic.

The IT Act, 2000 has failed to legalize electronic fund transfer in the country. The IT Act, 2000 does not recognize the concept of electronic payments, digital cash, electronic cash, electronic money or other existing systems of electronic payments and in its
absence, there can be no real boost for e-commerce in India. It is common knowledge that the growth of electronic commerce, without ensuring the facilitation of electronic payments, is not possible.

Electronic commerce is based on the system of domain names. The IT Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

The IT Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights in the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.

The IT Act mentions the use of electronic records and digital signatures in Government agencies. Yet, strangely, it further says in Section 9, that this does not confer any right upon any person to insist that the document in question should be accepted in electronic form by the government. The immense control of the government is apparent, as the Controller of Certifying Authorities has to discharge his functions subject to the general control and direction of the Central Government. The Internet and the
phenomenon of electronic commerce require that minimum hurdles and obstacles need to be put in their way. The IT Act, 2000 seeks to bureaucratize the entire process of regulating electronic commerce. This is likely to result in delays and other related problems.

Another basic problem relates to the language of Section 40 of the IT Act, 2000. Section 40 provides for generating key pairs in Chapter VIII dealing with the duties of subscribers. It states that where any Digital Signature Certificate, the public key of which corresponds to the private key of the subscriber which is to be listed in the Digital Signature Certificate, has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure. It may be submitted that the entire wording of Section 40 is faulty and has been shown in such a way as to denote that the acceptance of the Digital Signature Certificate precedes the generation of key pair by the subscriber. Further, how can a subscriber accept a non-existing Digital Signature Certificate, when the key pair is yet to be generated? The anomaly of Section 40 gets more pronounced, from the perusal of Section 41, which deals with acceptance of a Digital Signature Certificate. As such, the approach of Section 40 is technically incorrect. It is only after the subscriber generates the key pair that the public key can be handed over to the Certifying Authority. This has led to glaring fault under the IT Act, 2000. Further, the use of the word
‘shall’ under Section 40 of the IT Act further complicates the matter and promises to be a big hindrance in the actual growth of Digital Signatures in the country. It is also likely to impede the growth of e-commerce in the country. The IT Act, 2000 has left glaring loopholes in the digital signature regime that it proposes for the country. Cross-certification, as an issue, has not been comprehensively dealt with.

The IT Act, 2000 talks of Adjudicating Officers, who shall adjudicate whether any person has committed a contravention of any provisions of this Act or any rules, regulations, directions or orders made thereunder. How these Adjudicating Officers will adjudicate the contravention of the Act has not been made clear or well defined. Further, it has also not been specified as to how the Adjudicating Officers shall determine whether any contravention of the Act has been committed by any person outside India. Further, what authority would these Adjudicating Officers have vis-a-vis persons outside India who have committed any contravention of the IT Act, 2000, has also not been defined. No definitive procedure for adjudication by Adjudicating Officers has been exhaustively spelt out by the IT Act, 2000. Further, the territorial jurisdiction of the Adjudicating Officers and the Cyber Regulations Appellate Tribunal has not been defined.
Section 55 of the IT Act, 2000 states that no order of the V Central Government appointing any person as the Presiding Officer of a Cyber Regulations Appellate Tribunal shall be called in question in any manner and no Act or proceeding before a Cyber Regulations Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Regulations Appellate Tribunal. This provision is violative of the principles enshrined in the Constitution of India and, being not expedient, is likely to be struck down by the courts. The Central Government cannot claim immunity in appointments to Cyber Regulations Appellate Tribunal, as the same is contrary to the spirit and basic structure of the Constitution of India which embodies Judicial Review. Further, it may be submitted that if there is a defect in the constitution of a Cyber Regulations Appellate Tribunal, that goes to the root of the matter and renders all proceedings and acts of the Cyber Regulations Appellate Tribunal null and void ab initio.

Further, the IT Act, 2000 refers to any agency of the 17 government intercepting any information transmitted through any computer resource if it is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence. This is one provision, which is open to misuse by future governments to
suit their political motives as also for the purpose of victimization. No standards or provisions have been laid down by the IT Act, 2000, which define any conditions detailed above. The supporters of the cause of individual privacy and freedom see this provision as a gross violation of individual freedom and as unreasonable restrictions, which are not in sync with the rapid growth of Internet.

As Cyberlaw is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cover various kinds of cyber crimes and Internet related crimes. These include:-

a. Theft of Internet hours
b. Cybertheft
c. Cyber stalking
d. Cyber harassment
e. Cyber defamation
f. Cyber fraud
g. Misuse of credit card numbers
h. Chat room abuse
The IT Act, 2000 is silent on covering all kinds of offences dealing with abuses of chat rooms. Chat rooms are one of the most popular destinations on the net for the netizens. Chat rooms witness the unprecedented expression, in the written form, of dormant human feelings. Chat rooms give people an opportunity to express whatever they want to without any inhibition or fear because of the anonymous medium of Internet. The IT Act, 2000 covers none of the offences committed by people in chat rooms.

Another major grey area under the IT Act, 2000 is that it is silent on the issue of online credit card payments, misuse and misappropriation of credit card numbers online. To date, there is no law in our country, which gives legal recognition exclusively to credit card payments, in the manner like the recognition provided to negotiable instruments. As such, credit card disputes are covered by the various terms contracted between the subscribers and the credit card companies. Misuse of credit card numbers on the Net is growing daily. There is no provision mentioned in the IT Act, 2000 which deals with misappropriation of a person’s credit card number on the Net.

The IT Act, 2000 is completely silent about the availability or otherwise of the offences prescribed in Chapter XI. There is no categorical mention at any point in Chapter XI from Section 65 till Section 78 as to whether the offences prescribed under the sections
are available or not. This approach is very different from most other statutes, where the legislature takes pains to discuss the availability or otherwise of the offences. In addition, the IT Act, 2000 is silent on the fact of the concerned court which is competent to take cognizance of the offences detailed under Chapter XI of the IT Act, 2000. As the Act is completely silent on this issue, we have no option but to rely upon Part II, Schedule I of the Code of Criminal Procedure.

Another problem area in the IT Act, 2000 is that it does not apply its mind to the fact that the cyber offences or computer offences are specialized, white collared, technical and non-conventional offences which require a specific handling which is distinct from the handling of an ordinary offence in the real world under the Indian Penal Code. This is itself an area of major concern as it is likely, to open the floodgates of litigation. The IT Act, 2000 has adopted an inconsistent and disproportionate system of punishment, as compared to Indian Penal Code, 1860.

The casual nature in which cyber offences have been tackled under the IT Act, 2000 is also perhaps responsible for the fact that the IT Act, 2000 itself is totally silent on the issue whether the offences prescribed therein are compoundable or not. Consequently, one has no option but to refer to Section 320 Cr.P.C. Section 320 (9) Cr.P.C categorically states that no offence shall be compounded
except as provided by this section. Since, none of the offences mentioned in the IT Act find mention in Section 320 Cr.P.C, the cyber offences and computer related offences under the IT Act, 2000 become non-compoundable, by virtue of the operation of Section 320(9) Cr.P.C. Minor offences should have been categorically declared compoundable by the IT Act, 2000 itself. Since the provisions of Section 320 Cr.P.C are not in conflict with the provisions of the IT Act, 2000, the provisions of Section 320 Cr.P.C will be applicable to the IT Act, 2000, thereby creating a somewhat undesirable situation.

Another major grey area is that the draconian powers given to a police officer not below rank of the Deputy Superintendent of Police under Section 80 of the Act have been left untouched. Nowhere in the world is there a parallel-unrestricted power to any officer for the purpose of investigating and preventing the commission of a cyber crime. After all, the power given by the IT Act, 2000 to the DSP includes the power to “enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.” The power has been given without any restrictions of any kind whatsoever. It is possible that the same is likely to be misused and abused in the context of corporate India as companies have public offices, which would come within the ambit of “public
place" under Section 80, and companies will not be able to escape potential harassment at the hands of the DSP. This power has already resulted in the emergence of the practice of e-hafta (electronic hafta), as reported from some parts of the country. This area of the IT Act, 2000 promises to be one of the greatest concerns for the Government, the industry and the people at large. Section 89 of the IT Act, 2000 deals with the power of IV the Controller to make regulations. Section 89(2)(a) says that the regulations of the Controller may provide the particulars relating to maintenance of database containing the disclosure record of every Certifying Authority under Section 18(m). This is an oversight on the part of the legislature as Section 18(m) says that the Controller may perform the function of laying down the duties of the Certifying Authorities. Clearly, there is a mismatch between Sections 89(2)(a) and 18(m). The legislature ought to have mentioned Section 18(n) in Section 89(2)(a), as Section 18(n) states that the Controller may perform the function of maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public. This mismatch between Sections 89(2)(a) and 18(m) is bound to create problems for the Controller in making regulations in this regard and clearly needs to be amended.
Similarly, another area of mismatch is Section 89(2)(c). Under this provision, the Controller has been given the power to make regulations providing for the terms and conditions subject to which the licence may be granted under Section 21(3)c. Section 21(2) states that no licence to issue Digital Signature Certificates shall be issued, under Section 21(1), unless the applicant fulfils certain mandatory requirements. It is pertinent to note that Section 21(3)c says that a licence to issue Digital Signature Certificates, which is granted under this section, namely, Section 21, shall be subject to such terms and conditions as may be specified by regulations.

Firstly, it is amply clear from Section 21 that the license to a Certifying Authority to issue Digital Signature Certificates is not issued under Section 21 but under Section 24 of the IT Act, 2000. Section 21 only refers to any person making an application to the Controller for a licence to issue Digital Signature Certificates and that no license shall be issued unless the applicant fulfils certain mandatory requirements. The power has been granted to the Controller to grant a licence to issue Digital Signature Certificates under Section 24 of the IT Act, 2000.

There is a school of thought which states that the words “terms and conditions” specified in Section 21(3)(c) only relates to an applicant for a licence to issue Digital Signature Certificates
and that this interpretation is corroborated by the definitions provided in Section 2(g). Further, under Section 2(z), licences means a licence granted to a Certifying Authority under Section 24. As such, the conditions and conditions referred in Section 21(3) can only mean terms and conditions for the applicant for a licence. There is some confusion in the actual drafting of the IT Act, 2000.

Thus, technically and legally speaking, a licence cannot be granted under Section 21 of the IT Act, 2000 to any Certifying Authority to issue Digital Signature Certificates. A licence to any Certifying Authority can only be granted under Section 24 of the IT Act, 2000 which becomes more clearer from the definitions given in Sections 2(1)(g) and 2(1)(z). This is likely to create confusion, though it is clear that the Controller has the powers to determine the terms and conditions subject to which a licence may be granted to issue Digital Signature Certificates.

Another major grey area under the IT Act, 2000 relates to Section 89(2)(f). Section 89(2)(f) provides that the Controller may make regulations providing for the particulars of statements which shall accompany an application under Section 35(3). Section 35(3) states that any person making an application to a Certifying Authority for the issue of a Digital Signature Certificate shall also
annex, along with the application, a Certification Practice Statement or where there is no such statement, a statement containing such particulars as may be specified by regulations. Thus, Section 35(3) requires the mandatory submission of Certification Practice Statement by prospective users of Digital Signature Certificates to any Certifying Authority. This is an unheard of practice, in the context of Digital Signatures. Such a provision does not exist in any Cyberlaw in the world. The Digital Signature regimes in different countries only require the Certifying Authority to have their own Certification Practice Statement. It is neither possible nor perceivable for prospective applicants of Digital Signature Certificates to think about Certification Practice Statement, formulate the same and then ensure that their Certification Practice Statement accompanies the application for Digital Signature Certificate.

A user/subscriber cannot be required to submit a Certification Practice Statement. It is a Certifying Authority or an applicant for becoming a Certifying Authority who has to submit a Certification Practice Statement, or CPS, to the Controller under Section 22(2)(a). Section 22(2)(a) categorically states that every application for issue of a licence to issue Digital Signature Certificates shall be accompanied by a Certification Practice Statement. Further, the licence to act as a Certifying Authority can be issued by the Controller, only after the
Certification Practice Statement is submitted along with other mandatory requirements. The submission of the Certification Practice Statement is central to the entire process of licensing by the Controller.

In fact, the Certification Practice Statement is the bible for all procedures and processes to be followed by the Certifying Authority or the applicant. The Certification Practice Statement is inclusive of technical infrastructure, security, personal and employer considerations, physical security and other related parameters for the operation of the Certifying Authority's business. Auditors, approved by the Controller of Certifying Authorities, audit the Certification Practice Statement. The provision requiring an applicant for a Digital Signature Certificate, to submit his Certification Practice Statement along with his application for issue of Digital Signature Certificates, is the biggest impediment towards the growth and proliferation of the Digital Signature Certificates and the digital signature regime in the country. Till the time such a provision of law is amended by Parliament, this provision will continue to stand as a major impediment and no amount of executive orders or rules or directions, being secondary in nature, can override these mandatory requirements under Section 35(3) of the IT Act, 2000.
The Information Technology Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.

Another negative area of the IT Act is that the IT Act, 2000 does not provide anything relating to protection of data. The object of the IT Act, 2000, as is given in its preamble, is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as Electronic Commerce. It is pertinent to note that Section 2(1)(0) of the IT Act, 2000 gives a legal definition of the term “data” and a perusal of the entire law shows that data, as defined in Section 2(1)(0) of the IT Act, becomes the major subject matter of the various provisions of the IT Act, 2000.

However, despite data being so critical and crucial for the success of a legal infrastructure for promoting e-commerce and the information society, the IT Act, 2000 is completely silent on the issue of data protection. Not only is there no provision which provides for data protection or the penal consequences in case someone violates data protection privacy but even data privacy as a subject has not been touched under the IT Act, 2000. Thus, the Indian Cyberlaw suffers grossly due to the absence of any provisions relating to data protection and data privacy.
The IT Act, 2000 affords no protection of any kind for e-consumers, whose credit card numbers are stolen and misused online. It is also important to note that cyber fraud is not specifically covered under the IT Act, 2000 as a penal offence. At best, one can ask for damages upto Rs. 1 crore under Section 43 of the IT Act, 2000 if the person is able to prove the relevant requirements of Section 43 of the IT Act, 2000.

It is also pertinent to note that digital notarization and third party validation services have not been touched by the IT Act, 2000 at all.

Another grey area of the IT Act is that the same does not touch upon any anti-trust issues.

The most serious concern about the Indian Cyberlaw relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when Internet penetration in India is extremely low and government and police officials, in general are not very computer savvy, the new Indian Cyberlaw raises more questions than it answers. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the grey areas mentioned above.
II. SUGGESTIONS

India has got a very rich corpus of enacted laws. We possibly have one of the best and the largest number of laws in the world. The IT Act, 2000 is India's first step towards regulating the electronic medium and the electronic format. The law has only amended four different laws in the huge corpus of laws in our country. These four laws are The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 and the Indian Penal Code, 1860.

REQUIRED AMENDMENTS IN THE IT ACT. 2000

Various provisions in the Information Technology Act, 2000 require appropriate amendments. Section 3 of the Information Technology Act is a technology specific law in terms of digital signatures. At present, section 3 (2) prescribes asymmetric crypto system and hash function or Public Key Infrastructure as the only legally recognized technology for authentication of electronic records. There is a need for making the Information Technology Act a technology neutral law. Considering the fact that the UNCITRAL Model Law on Electronic Signatures, 2001 itself paves the way for technology neutrality, there is a need for making the present law, in tune with the existing realities of the day. There is a need for incorporating a technology neutral approach in the law. This can be in the form of an appropriate
provision by means of which other technologies, as specified by the Central Government, may also be used for authenticating an electronic record.

The cybercrime provisions in the Information Technology Act are neither comprehensive nor exhaustive. Further, amendments in the IPC, as made by the Information Technology Act, 2000 do not do justice of adequately covering all emerging cybercrimes. There is a need for strengthening the Information Technology Act in this regard by making appropriate amendments therein.

The Indian Cyberlaw makes the Controller Of Certifying Authorities as head of the digital signature regime in this country. Yet in Section 69 of the said act, the law has made the Controller of Certifying Authority the sole authority for directing any interception of any information transmitted through any computer resource. Such a provision is clearly not drafted in accordance with the overall scheme envisaged by the Information Technology Act.

Indian Cyberlaw also does not deal with various newly emerging Cybercrimes like cyber stalking, cyber nuisance, cyber harassment, identity theft, pretext calling and others. There is a need to come up with appropriate provisions under the law to deal with such newly emerging Cybercrimes.
Section 78 and 80 of the Information Technology Act provide for investigation of Cybercrimes, as stipulated by the Indian Cyberlaw, only by a Police Officer not below the rank of Deputy Superintendent of Police. I am of the opinion that the law needs to be appropriately amended as to ensure investigation of Cybercrimes based on competency of the Police Officer rather their rank.

Regarding extra territorial jurisdiction, Section 1 (2) and Section 75 of the Information Technology Act provide for the applicability of this law to any offence or contravention committed outside India, by any person. It is pertinent to note that the Indian Penal Code (IPC), as amended by the Information Technology Act, has been so amended as to incorporate, within its ambit, electronic records. However, the IPC is still applicable within the territorial boundaries of India only. There is a need for removing this disparity between the applicability and jurisdiction of the Information Technology Act and IPC. This is necessary so as to enable the law enforcement agencies to book perpetuators of crimes committed across boundaries, without ever physically crossing over the boundaries of India. Such an approach is further likely to assist the law enforcement agencies in their attempt of booking appropriate cyber criminals.

The Information Technology Act, 2000 only relates to information or data residing in a computer, computer system or computer network. It does not deal with the question of electronic information when it is in
transit within a network. The issue relating to legal regulation of data traffic needs to be duly incorporated so as to cover legal and regulatory issues relating to information in transit between computers, computer systems or computer networks. In this regard, it will be relevant for India to look at the definition of data traffic as recommended by the Council of the Europe Convention on Cybercrime. It will also be prudent for India to amend Section 66 of the Information Technology Act to incorporate aspects relating to information in transit.

Section 70 of the Information Technology Act deals with declaration of any computer, computer system or computer network to be a protected system, however, there is no definition of the term "protected system" and there is a need for amending the law so as to not only provide for such a definition but also provide for the various criteria based on which a system could be declared as a protected system.

The Indian Cyberlaw has not taken any specific stand on encryption. Section 69 (2) of the Information Technology Act is a law about decryption of information. There is a need for taking a definitive stand on encryption. This can be done in the same manner as in which United States has gone about regulating encryption. Considering the fact that encryption today plays an important role in security of data or information, there is a need for Indian Cyberlaw to disclose its
stand on encryption and not lead to a situation of confusion where different systems are followed.

Section 79 of the Information Technology Act is entitled "Network Service Provider not to be liable in certain cases". However, what is the extent of liability of such Service Providers has not been specified by the said provisions. There is a need for law to provide clear liabilities and rights of Network Service Providers including intermediaries. Such provisions clearly put an enormous burden on Network Service Providers and virtually makes them liable for all third party information or data, made available by them, even in cases where they come within the exceptions stated therein. These exceptions are very hard to prove and would involve a lot of confusion. It is imperative for the law to come up with more clarity on this issue.

The law has put enormous burden on proving printouts of electronic records as evidence as is dealt by Section 65A and 65 B of the Indian Evidence Act as amended by the Information Technology Act, 2000. The practical working of the law has demonstrated that it is extremely difficult for any citizen or users of the computer to fulfill the requirements of proof of printouts or computerized records as stipulated by the Indian Evidence Act.
There is a need to come up with appropriate relaxation in such a manner so as to ensure that while the manner of proof shows the preservation of veracity and authenticity of information contained in the computer, yet it does not place an unrealistic and enormous burden of proof on a genuine computer user so as to defeat the cause of justice.

While the law talks about proving of digital evidence, the law does not provide any mechanism for examining the document in question. It will be important for the Indian Cyberlaw to come up with creation of appropriate mechanisms to examine questions relating to digital evidence.

The Indian Cyberlaw does not talk about either electronic records or online dispute resolution mechanism. There is a need for amending the law to make appropriate provisions in this regard.

The Information Technology Act, 2(xx) needs to be further amended so as to provide for specific provisions stipulating for mandatory audit of Certifying Authorities. In addition, the law needs to be further amended so as to incorporate thereunder provisions relating to cross certification of Certifying Authorities.

Clearly, a number of other legislations need to be passed urgently in order to enable India to take an effective plunge in the e-commerce
revolution. A perusal of various laws and their analysis makes it clear that the Government has to take appropriate steps to legislate in the following areas so as to further develop the legal infrastructure in the context of the electronic environment:

1. Intellectual Property Rights Protection including Copyright, Trademarks & Patents
2. Protection of e-Consumers
3. Electronic Payments & Electronic Fund Transfer
4. E-Banking
5. Freedom of Information
6. Electronic Archival
7. Data Protection
8. Cyber Crimes Code
9. Trade Automation
10. Anti Piracy
11. Privacy Protection
12. Right for Information

STRENGTHENING OF CRIMINAL JUSTICE ADMINISTRATION
The dynamic nature of computer technology, compounded by specific considerations and complications in applying traditional laws to this new technology, dictate that the law enforcement, legal and judicial communities must develop new skills to be able to respond adequately to the challenge presented by computer crime. The growing sophistication of telecommunications systems and the high level of expertise of many system operators complicate significantly the task of regulatory and legal intervention. Growing familiarity with electronic complexity in the general population coupled with the comparative level of ignorance amongst existing law enforcement agencies is contributing to the spurt in cybercrimes. Therefore, there is an urgent need to educate these agencies about the complex computer techniques so as to make them competent in enforcing the law. Law enforcement agencies, legal and judicial communities need to develop minimum level of skills and expertise to understand the complexities of the computer networks and modern telecommunication systems so as to effectively deal with their possible misuse.

Till recent times the computer crimes were mainly limited to the economic environment and in response to this the enforcement agencies have provided training to their personnel dealing with economic crimes like frauds embezzlements etc. However, with the Internet revolution gripping the entire populace of the world, cybercrime has grown beyond economic crimes and reached all the
forms of traditional crimes including drugs and women trafficking, industrial and military espionage etc. as we have already seen from the preceding chapters. Therefore, the expertise and training cannot be limited to any group of personnel in the enforcement agencies but has to be across the organisations.

The United Nations has identified the five areas in which the training has to be given to all the members of judicial administration and enforcement agencies.

They are as follows:

- **The difference between a civil wrong and a criminal wrong:** Since all the computer related abuses may constitute a criminal offence, it is necessary to be able to differentiate between civil wrongs and criminal wrongs as well as to determine what are merely social nuisances. This process of criminalization and differentiation is necessary to establish liability and respect the rights of citizens and also to permit proper utilization of scarce resources of enforcement agencies in conducting investigations into deserving incidents of cybercrimes.

- **The technology:** Instead of limiting the technological training to any particular departments, the police should introduce computer trainings to all its personnel involved in crime
detection and prevention. It is often seen that the help from outside experts are not very useful in dealing with cybercrime detection and it is necessary to have investigators with not only solid criminal investigation backgrounds but also supplementary technical knowledge. Similarly, all those who fulfill the prosecutorial and judicial duties also must possess enough technical knowledge to be able to properly prosecute and adjudicate computer crimes.

- Proper means of obtaining and preserving evidence and of presenting it before the courts: Computer technologies, with their stress in paperless atmosphere, has introduced serious challenges to the traditional systems of evidence collection and production based on evidence that is tangible and detectable by human senses. It is imperative that the legal regime dealing with evidence must be reformed so that investigators are able to search for, gather, analyse, maintain the continuity and integrity of, and present computer evidence for the purpose of judicial hearings' in a manner that is 'fair to the parties concerned and that does not risk damaging or modifying the original data.

- Intricacies of the international nature of problem: In gathering evidence the investigator must be able to understand and deal with international issues, such as extradition and
mutual assistance. For this purpose, the investigator may require a fair understanding of the laws of evidence, criminal procedure and data protection of other jurisdictions while pursuing international investigations into cybercrimes.

- Rights and privileges of the accused and victim: Another area that the UN identifies as requiring training programme, is the sensitization of the criminal justice administration towards the rights and privileges of the parties involved in cybercrimes. This is required, as the credibility of enforcement agencies in various jurisdictions will depend upon their equitable application of law, especially when the parties involved are from different jurisdictions. This will also help in building the confidence of the people in general in the administration so that victims of cybercrimes come forward with information.

HARNESSING INTERNATIONAL CO-OPERATION

Time and again we have reiterated that with advent of the Internet, the criminal have overcome the national boundaries that hindered them in the past, in their activities. Only way to deal with this phenomenon is to increase effective international cooperation. Harmonisation of criminal and cyber laws and cooperation among international community are the needs of the time. The efforts that were initiated by organisations like OECD, UN, Council of Europe etc are noteworthy.
The Convention adopted by European Council institutionalize the international cooperation with its provisions for establishing 24x7 networks etc amongst member countries for the exclusive purpose of providing timely assistance to other countries in preventing and detecting cybercrimes.

These efforts need to be taken to a logical conclusion with a truly international Convention on cybercrime. Various private and academic institutions have come out with draft agreements in this regard. For example, Stanford University, Hoover Institution, in California, organized a Conference on International Cooperation to Combat Cyber Crime and Terrorism in December 1999 and a proposal for an International Convention on Cyber Crime and Terrorism has been introduced in August 2000. Among the International Law Enforcement agencies, Interpol hold its First Interpol Training Seminar for Investigators of Computer Crime in 1981. This Seminar was followed by International Conferences on Computer Crime in 1995, 1996, 1998, 2000, and 2003.

Much more needs to be done in this regard if the world wants to deal effectively with the cyber criminals. In January 2000, US Attorney General challenged National Association of Attorneys General and other state and local law enforcement groups to make it a priority to respond to these significant needs and suggested immediate adoption of following measures:
• Create a 24-hour cybercrime point of contact network, where each participating federal, state, and local law enforcement agency would provide a designated contact who is available 24 hours per day, 7 days per week to assist with cybercrime issues. This contact could be available via a pager system or coordinated through a centralized "command center."

• Create an online clearinghouse for sharing information to avoid duplication of effort and multiple investigations of the same unlawful conduct. Existing mechanisms, such as XSP, LEO, or Consumer Sentinel, may either serve this function or serve as building blocks for such a service.

• Develop conferences for all state and local Internet investigators and prosecutors, yearly or bi-annually, at which recent developments are discussed case progress shared, and networks reinforced that will facilitate state, federal, and local cooperation.

• Develop additional policies and mechanisms to enhance cooperative interstate investigative and prosecutorial capacities and encourage coordination among their constituents.

Though she was speaking in the context of US Federal and States administrative system, these steps are very much pertinent to the international cooperation among nations too.
However, when one country's laws criminalize a crime and another
country's laws do not, cooperation to solve that crime, as well as the
possibility of extraditing the criminal to stand trial, may not be
possible. Generally, the requirement of dual criminality is considered
necessary for international cooperation in criminal matters including
extradition and search and seizures. Municipal courts often refuse to
recognize or grant permissions where the alleged act is not an offence
within its territorial jurisdiction. Therefore, inadequate regimes for
international legal assistance and extradition can shield criminals from
law enforcement: criminals can go unpunished in one country, while
they thwart the efforts of other countries to protect their citizens. So
any effective cooperation amongst the nation States will only become
possible when there is at least some meeting ground in their respective
national laws dealing with cybercrimes. The following
recommendations on legal measures to be adopted for preventing
misuse of international data networks made by P8 Expert group, way
back in 1997, is still pertinent in this regard.

- Strengthen International mechanisms for addressing illegal
  actions, e.g., by creating a well defined set of international
  minimum rules against illegal actions, such as hacking,
  computer espionage, computer sabotage, computer fraud and
  copyright infringements.

- Strengthen international mechanisms for addressing illegal
  contents, e.g., by creating a well defined set of international
minimum rules for illegal contents to be prosecuted and punished worldwide, especially with respect to child pornography, bestiality, the glorification of violence, hate speech as well as defamation of minorities and individual persons.

- Encourage countries to define an adequate system of rules for the responsibility of Internet access providers and service providers, e.g., by creating a legal system so that in all countries service providers must undertake reasonable efforts to erase illegal contents on their servers when made aware of these contents, while at the same time, the free flow of data should not be hindered by attempts to block access to other servers and by holding access providers liable.

- Encourage countries to establish national laws for the effective prosecution of computer crimes, especially with respect to search and seizure of computer systems and international networks, duties of witnesses (e.g., to provide passwords or to decrypt files), wire tapping and accessing computer systems.

- Address possible abuses of anonymity, and install an international system for lifting anonymity in cases of abuse, thereby requiring adequate legal safeguards for privacy rights (e.g., by demanding court orders as a prerequisite for transferring specific data to the prosecuting authorities), thereby considering the fact that lifting anonymity is only
possible, if all countries co-operate, which are crossed by communication.

- Develop an international information network and other information systems with respect to the prosecution of illegal and harmful practices detective on the Internet.
- Foster Co-operation amongst law enforcement agencies with special respect to urgent measures for freezing data in international search and seizure procedures.
- Clarify issues of Jurisdictions Educate, and train Law Enforcement Agencies about cybercrimes and its prosecution.

If the world is to overtake or at the least, catch up with the cyber criminals it has to think and act, as one. Isolated national and regional efforts in combating cybercrimes have only limited value, due to the inherent characteristics of the cyber world. Therefore, there should be coordinated efforts among nations to streamline the entire strategy in this regard. The suggested steps in the 'way forward', in combating the menace of crime in cyber world is summarized as follows:

- The mindset based on criminalisation, as the solution for all ills plaguing cyberspace, must be changed. Alternate strategies must be adopted in limiting the growth of cybercrimes.
- Technology ought to be considered as a viable response to limiting cybercrimes.
• Awareness and capacity building among all strata of the society must be pursued. This must receive more thrust as far as law enforcement agencies are concerned.

• Role of parents and teachers in moulding the cyber behaviour of future netizens must be given adequate thrust.

• Information Technology must be projected and accepted as a part of critical infrastructure and accordingly, effective and adequate responsibilities must be built in.

• Cybercrime is not a static concept. Accordingly, legal response must be dynamic and ongoing legal reforms must be facilitated.

• Selective criminalisation in cybercrime regulations and their strict enforcement and implementation warrants more thrust and insight.

• Focus on international efforts in harmonization and coordination of efforts must be increased.

Finally, all the necessary attention must be given and activities coordinated, by the society in general and the technologists, academia and administrators in particular, to limit the influence of criminals in cyberspace and to exploit the IT revolution for the upliftment of the entire society.