CHAPTER 8: CONCLUSION

From the beginning of the civilization there has existed some mode of communication, between the individuals in the society. As the civilization developed these modes of communication also changed. Human being strives for better, and ways of adopting new modes of communication is no exception to it. Before speech was introduced, gestures were used as a mode of communication. By passing of time speech became the second mode of communication. Then came writing and it brought into existence series of laws in written form. The Internet is still in its early stage of development. As it is the new mode of communication, we need more efficient laws to govern this mode of communication. As the Internet grows, the laws laying down regulations as to Internet are also in the developing phase. From 'gestures' to 'Internet' man had went a long way in its search for excellence.

The Internet is probably the largest of the open networks, which now form a disperse global entity. The notion of physical territory is necessarily foreign to the technical norms governing the Internet--instead, the standards and protocols of Internet communication have developed in such a way as to go beyond the limits of geography and politics. Unfortunately, the Internet does not lend itself well to a constitution in the normal sense of the word. Unlike a nation-state, it has no identifiable territory. Its citizens, on whom a democracy might be based, are not easily identified. It does not have the same concerns as a nation-state.

It is submitted that, there are fundamental inconsistencies between government of any kind and the global computer network-of-networks known as the Internet. The essential feature of the Internet is lack of central control. It is quite apparent, that efforts to regulate Internet at global level have failed completely. Thus, while the existence of rules and regulations as a basis for regulating the Internet would be an interesting subject for debate, the exercise has little practical application. Due to the nature of the Internet, including its

history, culture, and universality, its effective regulation is quite impossible. The decentralized structure of the Internet, spreading out from the ARPANet/NSFNet backbone, allowed easy expansion, as did the evolution of a communications standard that was widely compatible with different computer networking software. Transmission Control Protocol and Internet Protocol (TCP/IP), which is the basic form of the standard, continues to link computers into networks, and networks into the Internet as on today's date. The TCP/IP software was public domain, and decentralized and anarchic by its very nature, and therefore it is difficult to stop people from barging in and linking up. Thus, the Internet was hardly planned at all. Mostly, it just happened, as first scientists, then academics and finally the general public began taking advantage of its tremendous capacity for connectivity and communications.

Below mentioned are some special attributes of Internet, which make the cyber crimes different from conventional crimes like murder, rape and kidnapping. They are:

- Internet doesn't respect geographical boundaries. Cybercriminals sitting in one corner of the globe can commit crime and its impact may be felt in another part of the world. Cyber criminal would be almost invisible when he commits cyber crime.
- Secondly, cyber crimes are committed in cyberspace, i.e. the cyber criminal does not come face to face, nor is he physically present at a place where the effect of the crime takes place.
- Cyber criminals are well equipped with technological aspects. Their weapon is technology and not knife or pistol.
- Due the aforesaid features of Internet it is difficult to collect evidence and to do necessary investigation. At the same time, the commission of the cyber crimes is very swift. It takes only a few minutes to introduce virus into a computer systems or to play on line frauds.

While many of the countries are in the process of enacting cyber laws, India is one among the luckiest to have one. Union Government deserves unqualified praise for responding to the cry of the nation. Apart form India countries like USA, Canada; Singapore etc have also enacted cyber laws. The Information

technology Act 2000, no doubt is a good piece of legislation. It is based on the UNCITRAL Model Law on Electronic Commerce. The Act is basically E enabling and aims for recognition of digital signatures among other things. The Information Technology Act 2000 (IT Act 2000) neither defines 'cyber crime' nor uses this expression, but only provides the definition of, and punishment for certain cyber related offences.

Cyber crimes such as **Hacking, virus launching etc.** are the most serious offences that mankind is facing today. Virus programmes such as Melissa and Love bug had cost loss in billions. The recent incidents of hacking the websites like Yahoo.com, Amazon.com have created doubt on reliability of Internet in the minds of netizens. Cyber crimes are growing at an alarming rate and have become rampant. It must be realized that everyone and not just netizens is a potential victim. Section 66 of the Information Technology Act 2000, reads:
"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in the computer or diminishes its value or utility or affects it injuriously by any means ...commits hacking".

Like all criminal offences, hacking also requires mens-rea i.e. intent or knowledge, and actus reus. It is apparent from the definition that innocent errors of omission or commission, which may destroy or delete any information in a computer, or diminishes its value or utility would not amount to hacking. The intent to commit the offence is a question of fact to be gathered from the circumstances of each particular case.

Hacking under section 66 of the IT Act has been very widely defined, which is much wider then the concept of the hacking as understood in the common parlance i.e. breaking into computer systems. Though the definition does not talk of "breaking into computer systems", it says: "destroys or deletes or alters any information residing in a computer resource or diminishes its value." Even launching of virus in a computer system would amount to "hacking". The legal definition of "Hacking" in India is defined in such a way that, hobbies of

hacking, defacing or tagging, would also be covered within the ambit. Hacking being one of the most prevailing cyber crimes can be combated only via strong deterrent legal measures and sound technological backbone. Cyber crimes are committed through technological edges, and therefore to combat it we need to have efficient software's, which can prevent breaking into computer system. It is submitted that Indian legislatures, by using broad terminologies in S. 66, has done praiseworthy task.

Virus is a man made programme which can alter or destroy the digital information. Section 43 C of the Information technology Act 2000 deals with the offence of Virus launching. However, the section is silent on the corporeal punishment and it imposes just monetary liability. It is submitted that along with monetary liability some corporeal punishment must also be provided so that it will carry a deterrent effect. Further ---the act of planting virus will also fall under Section 425 of Indian Penal Code, which deals with the offence of Mischief. The Indian Legislatures, by using broad terminologies in S.66 has done a commendable task.

Today, **Cyber pornography** has become rampant on the Internet. It is difficult to regulate because different countries have differences in acceptable limits of morality. Society recognizes that some forms of communication that are suitable for adults are not suitable for minors who lack maturity and emotional development. It is found that exposure to cyber pornography is against the goal of healthy development of children who are the future of any nation. With Internet one can have access to pornographic material at the click of the mouse. Further, many of the web sites provide free excess to such objectionable content that very much disregards the age criteria for viewing such content. Recognizing the ease with which minors can use the Internet to access pornography, attempts are made at global level to prevent the ease availability of sexually explicit material on the Internet. In this context Section 67 of the IT Act 2000, which deals with Publication of information, which is obscene, needs attention.

Though the Section is very nicely drafted it has some grey areas. Section 67, which punishes the publishing and transmission of obscene material in electronic form with imprisonment of upto 5 years along with a fine of upto 1 lakh on first conviction, and with imprisonment upto 10 years with a fine upto Rs. 2 lakh on second or subsequent conviction, is controversial provision in law. The words "...is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it" in section 67 have been borrowed form section 292 of the Indian Penal Code 1860. However, it is found that specific nature of Internet makes the words of the Section 'a dead letter'. For e.g. if some friends are discussing on sex, then in such case law cannot not interfere, as it would amount violation of their right to privacy. But, if on Internet you are enjoying sex chat in the chat room then section 67 will come into play. In such case it will lead to violation of the right to privacy. It is submitted that the application of Section 67 should have been limited to the cases in which obscene material is transmitted to persons below 18 years of age. Lastly the original creators of pornographic web sites, and those who send pornographic material over the Internet, must be labeled as criminals.

The arrest of juvenile – a 16 year-old boy of Air Force Bal Bharti School of New Delhi-for committing the offence under section 67 i.e. launching of a web-site which contained obscene material about girl student, has given rise to certain questions such as, whether strict action should be taken against the boy, and, isn't posting lascivious material on the web site distinct to writing of offensive material on toilet walls. It is submitted that, the action taken against the accused should be harsher than against a poor juvenile caught for stealing. The way media reacted to that arrest, and the action taken by school authorities, were necessary for serving as a deterrent to the accused and juveniles who share similar ideas. Posting of offensive material on Internet is more serious offence than painting or writing obscene stuff on toilet walls. The reason is a web site is accessible on a few clicks to the whole world, whereas a toilet wall is available only to few individuals. Thus, the only protection against this menace is the strong technological backbone. Enacting of the legislations enough will

not go help us lot. It is humbly submitted that for protecting children's form obscene material available on net, filtering software's may go a long way apart from stringent legislations. While these are valid solutions, they do not necessarily work. One solution that may really work is the creation of adult-oriented top-level domains (TLDs). In its most simple way, the TLD is the identifier that comes after the 'dot' in all Internet addresses. For instance, in the Internet address 'yahoo.com', the 'yahoo' is the second-level domain and 'com' is the top-level domain. From the viewpoint concerning children, the new top-level domains such as ". xxx" or ". sex" would make it much easier for filtering devices to block pornographic materials. Instead of the keyword, the filtering device could focus on the site's top-level domain. If nothing else, it would make it easier and therefore maybe more likely for parents to identify and monitor the sites their children visit on the Web.

Along with different cyber crimes, **Defamation and Cyber stalking** have also become rampant. Internet provides a good platform to people to express their views, but at times it is also being misused. It is a sad state of affair that the Information Technology Act 2000, does not deal with defamation and cyber stalking. In absence of the statutory definition we have to depend on the provisions laid down in Indian Penal Code (IPC). If an e-mail is innocently worded, it would not be treated as criminal threat under the IPC. Therefore it is submitted that the term should have been defined and made punishable under the IT Act 2000. Our legislatures may define the term keeping in line with the definition given in Cyberstalking legislation passed in the U.S. and Canada so as to keep a check on this problem. Thus, the peculiar characteristic feature of the Internet makes it easy for the wrong doer to escape away with. To combat the cyber crimes, legislation itself is not enough. Along with this, we need responsible members in the society who can act as teacher, friends and policemen to guide minors and adolescents.

The growth of Internet has brought with it new legal issues. **Right of Privacy** has become a burning topic in today's era of Internet. In today's digital environment the earlier concept of right of privacy i.e. 'right to be let alone' has become obsolete. Today personal information can be transported and

distributed around the world in seconds. With the growth of new technology society and governments is also recognizing its importance. Section 72 of the Information Technology Act 2000 deals with Penalty for breach of privacy. It says: "Save as otherwise provided in this act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punishable with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both". Further, the act of interrupting with the personal data of the person without his consent will also fall under the broad definition of Hacking. In Canada, there is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms. However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognized an individual's right to a reasonable expectation of privacy. Privacy is regulated at both the federal and provincial level. In the USA, The Privacy Act of 1974 protects personal information held by the federal government by preventing unauthorized disclosures of such information. Individuals also have the right to review such information, request corrections, and be informed of any disclosures. The Freedom of Information Act facilitates these processes.

No doubt, privacy on the Internet is in a fragile state, however, there is new hope for its revival. Crafting proper privacy protections in the electronic realm has always been a complex attempt. It requires a keen awareness of not only changes in technology, but also changes in how citizens use the technology, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reconsider our fabric of privacy protections. In an environment where there are no proper legislations, the only protection against the violation of right of privacy over Internet is strong technological backbone.

Internet has brought with itself most debatable issues that the society has ever faced, i.e. **Jurisdiction of the courts**. Internet, which fully disregards the geographically boundaries has raised a novel issue of jurisdiction of courts. While there are on-line cross border dealings, the question that arises is which court would have jurisdiction to resolve the on-line disputes. From this question another important question follows and that is, what is the legality of the present rules relation to jurisdiction of the courts. Under such confronting questions can we assume that existing rules relating to jurisdiction of courts are not applicable to on-line disputes? Legal communities at global level have challenged the present law of jurisdiction of courts on grounds of hardships that websites may have to face and the uncertainty in the decisions of the courts on the question of applicability of rules of jurisdiction.

At this stage it becomes important to understand that, Internet is a global network, which provides to every individual (apart form his nationality, caste or gender) a facility communicate or to do business at global level. There are chances that the website has to face lawsuit in the foreign courts, but that is due to the fact that Internet is globally accessibly. Infact, it is this characteristic of the Internet that actually leads the websites to defend the suits in foreign courts. Under such circumstances it is found that one cannot blame the principles of jurisdiction. Much depends upon whether the website is active or passive. In cases like Bensusan Corp. v. Burger king courts have held that merely creating a website does not give rise to jurisdiction at global level. Thus it is the global nature of Internet that gives rise to global implications. Those who do business on-line are like Multinational Corporations who must regulate their actions in harmony with laws of different countries. Thus Hindustan Liver Ltd. cannot say that they will do business in India, but will not abide by the Indian Consumer Protection Act, and instead would like to be governed by the laws of the country where their offices are based. So, it is the very nature of the Internet, which will lead to global implications, and not the law of jurisdiction. It is true that present law of jurisdiction has failed to resolve on-line disputes, but still it remains the fact that law is unfailing and feasible for

determining the place of suing in cases of cybercrimes. Most of the decisions of the courts relating to jurisdictional disputes are rational. It is also true that there are certain peculiar problems in deciding jurisdiction of courts in case of on-line disputes. But these are just preliminary problems, which is bound to arise due to changes in society.

Thus it is submitted that, Section 1 and Section 75 in the Information Technology Act 2000, which deals with the applicability of the IT Act is very rightly drafted. Looking to the special characteristic of Internet, our legislatures have rightly given the long-arm effect to the section. At the same time there are certain grey area, which needs focus. For e.g., though the statute is apparently a 'long arm statute', it does not indicate the powers of the adjudicating officers when a person commits a cyber crime outside India. Apart from this, some practical difficulties on the topic of extradition to bring cyber criminal to India may also arise. The Internet has brought a revolution, which is significantly altering our lives and the way we communicate. In this background, it is submitted that the present law of jurisdiction has served it purpose very well. Initial small problems in the application of the law must not influence to reject our laws of jurisdiction. Even if there are any criticisms, it may be directed towards the application of the law by the courts but not the law itself. There are bound to be some inconsistencies in any legal systems. But, these should not be a valid reason for discarding our laws of jurisdiction. Jurisdiction follows the acts, and therefore, if the acts are global, jurisdiction also becomes global. Thus the Indian law of jurisdiction, at present is fair and a few uncertain decisions cannot dismiss the law of jurisdiction itself.

Section 43 of the act deals with **Penalty for damage to computer, computer system, etc.** It provides for compensation to the aggrieved party not exceeding one crore rupees. This provision for payment of compensation in terms of money only may not have deterrent effect upon the wrongdoers. In order to have deterrent effect what is further required is a provision for imprisonment along with fine payable by the accused. Further, under section 44 of the Act, provision is made for penalty for failure to furnish information, return etc. and the penalty prescribed under the section is payment of penalty

not exceeding 10,000 rupees for every day during which failure continues. No provision for imprisonment is prescribed under S.44 of the Act. Even Section 45, which deals with residuary penalty for the violation of any rules or regulations (for which no penalty has been separately provided), imposes liability to pay compensation not exceeding 25,000 rupees, but it omits to provide for imprisonment of the accused who is found guilty. The general view is that when punishment only by way of fine is provided the rigors of the law is reduced to a considerable extent because in modern times payment of fine is not perceived as effective punishment. Therefore it is submitted that under all the three sections i.e. S.43, 44, and 45 punishment by way of imprisonment must be provided.

Section 49 of the Act deals with the **Composition of Cyber Regulation appellant Tribunal**. It provides that a Cyber Appellate Tribunal shall consist of one person only, referred to as the Presiding Officer of the Cyber Appellate Tribunal to be appointed, by notification, by the Central Government. Regarding the qualification for appointment as Presiding Officer of the Cyber Appellate Tribunal, Section 50 says:

- he is, or has been, or is qualified to be, a judge of a high court, or
- is, or has been, a member of the Indian Legal Service and is holding or has held a post in Grade I of that service for at least three years.

What seem to be objectionable over here is the qualification as well as the composition of the Tribunal. It is submitted that the position would have been better if the Tribunal consists of one presiding officer and two-member i.e. a total of three people. From among, one of the members must be entirely from the field of I.T. One out of the remaining two (leaving aside the presiding officer) should be strictly from legal / judicial background and the third having experience of both I.T. & legal field. Further while appointing the presiding officer every effort should be made to select a person who has some background of I.T. as well.

Section 46 of the IT Act deals with **Power to Adjudicate** – It says -

(1) for the purposes of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under the Central Government shall, subject to the provision of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in manner prescribed by the Central Government.

2) * * *

3) No person shall be appointed as an adjudicating officers unless he possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government

4) * * *

5) * * *

A joint reading of sub-section 1) and 3) makes it clear that the Act prescribes that no person should be appointed as an "Adjudicating Officer" unless he possess such experience in Information Technology and legal or judicial experience as may be prescribed by the Government. Further, he must not be below the rank of a Director to the Government of India or an equivalent officer of the State Government. At this stage it becomes important to have a look at the pecuniary jurisdiction provided to the Adjudicating Officer under this Act. The Act prescribes for financial penalty i.e. upto one corer rupees (S.43). This indeed is a praiseworthy attempt to bring at least some relief to the aggrieved. The Adjudicating Officer has powers to award punishment upto 10 years of imprisonment and fine upto one corer rupees. Those who say that the powers vested to the Police Authorities under this Act are "Draconian" must consider the likelihood of abuse of powers by one of the many adjudicating officers who may be operating under the system. Inspite of the fact that, provision of appeal is laid down in the Act, the damage that an inefficient adjudicating officer may inflict on innocent Netizens, or cyber cafe owners could be intentional. The Act does not specify any checks and balances to prevent misuse of the powers of the adjudicating officers. On the other hand, Section 84 provides protection from legal action to the adjudicating officer for acts done in good faith. It is found that these provisions are drafted very loosely. Further these provision

need to be reviewed and a proper system for appointment, transfer, and removal of the adjudicating officer need to be provided. It is submitted that one of the solutions to this problem is to see that all enquires will be held in the presence of an 'Expert Committee' which may consist of at least three members with requisite knowledge of law and information technology. This committee can be created from group of talented persons created for the purpose with the assistance of the Cyber Regulation Advisory Committee. The member of this committee should record their comments independently in a confidential report to such authority which can be referred to in the event of necessity and when an appeal being heard.

According to **Section 82,** which deals with **Deemed Public Servants,** all officers of the Cyber Regulation Appellate Tribunal and the Office of the Controller would be deemed as "Public Servants under section 21 of Indian Penal Code. This clause does not include the Adjudicating officer. It is submitted that the public servant definition should be linked to the definition in the "Prevention of Corruption Act" and not with Indian Penal Code. This change may help to put more check on any misuse of powers.

Regulation of **Intellectual Property Rights,** particularly copyright on the Internet is an ever-growing problem. The Act does not discuss the implications of any copyright violations over the net. It has no provisions to penalize copyright infringers. Internet piracy is a major problem has not been tackled by this Act. It is submitted that necessary amendments be made in the Indian Copyright Act so as to penalize the wrongdoers.

Under **Section 80** of the Act, police officers not below the rank of Deputy Superintendent of Police authorised by the Central Government have been given wide **powers to search and arrest persons without warrant** who has committed or reasonably suspected to have committed or about to commit any offence under the act. It is submitted that, these powers seem to be very wide, and hence, there should be some monitoring mechanism to ensure that no excesses are committed.

Under the Act various provisions are made for imprisonment and fine, but the Act fails to provide which concerned judicial authority i.e. court can impose such imprisonment and fine. If we take a short look to Criminal Procedure Code, then section 6 of the Code deals with the different kinds of the courts such as Judicial Magistrate First Class, Metropolitan Magistrate, and Court of Sessions etc.
Further Criminal Procedure Code also provides for the jurisdictional powers that such courts possesses,

1. High court and the court of sessions can pass any sentence of imprisonment and fine. (however, death sentence passed by the sessions court shall be subject to the confirmation of the High Court)
2. Chief Judicial Magistrate can pass any sentence authorised by law except the sentence of death or imprisonment for life or imprisonment for term not exceeding 7 years.
3. Judicial Magistrate First class can pass sentence not exceeding 3 years or fine not exceeding 5000 rupees or both.
4. Court of Magistrate of Second class can impose sentence for not exceeding 1 year and fine not exceeding 1000 rupees or with both.

Now let us take a look to section 66 of the IT Act, which deals with 'Hacking with Computer System'. The section says "whoever commits hacking shall be punished with imprisonment upto three years and fine which may extend upto 2 lakh rupees or with both." Now, if the case is tried by JMFC court the offender can be sentenced upto 3 years, but the court cannot impose penalty by way of fine for more than 5000 rupees. Thus the act fails to provide necessary provisions for the concerned authority that can try a case and impose necessary imprisonment and fine.

The IT Act is a comprehensive piece of legislation, which aims at policing some of the actions over the Internet. The fundamental approach of the Act is towards validating and legalizing E-commerce. Due to this business transaction costs will be reduced and transaction will multiple. Cyber Crimes will hopefully be curbed and offenders will be strictly penalized. Policing these crimes is extremely necessary. At the same time the police officers who are vested with wide powers under the IT Act must also be educated in computers and Internet. This would help them in executing their powers effectively and efficiently. But in

order to curb computer crimes, the police alone cannot make all the difference. Awareness regarding these cyber laws must be created. Private and Non Governmental organizations must play an active role in communicating this message to the masses. Moreover, the judiciary will also have to play a positive role in adjudicating cyber trials. Co-ordination amongst the organizations, police and judiciary will definitely create some impact and minimize the crime rate. However, the working and implementation of this law will depend greatly on the rules and regulations that will be formed by the Government and other authorities constituted under the Act.

This Act is not the end but only a beginning. It leaves various issues untouched, some of them relating to intellectual property rights (Patents, Copyrights and Trademarks), data protection and taxation. No concrete regulations have also been formulated for cross border issues. These issues are of immense importance and the Parliament must speedily frame laws to govern them. While legislation will always be lagging behind as time and technology progress, the Parliament must ensure that it keeps amending the law and enacting new laws to keep pace with ever-changing standards. At the same time, Indian law must be consistent with international standards that are prescribed and that may be prescribed in the future. This is essential if we desire to effectively regulate this boundless world.

India is amongst few of the countries in the world, which have any legal framework for e-commerce and e-governance. Indian industry projections indicate that business transactions over the net would cross Rs. 4500 crore (Rs.45 Billion) by 2004. The correct and honest implementation of this Act would definitely be a boon to the Indian InfoTech Sector. The Act has been passed at a time when the Internet population in India is low and therefore it is hoped that implementing the law should not be very difficult. The Act is a good march forward to keep pace with the changing time. There is still a long way to go. Times ahead promise to be very interesting.