SUMMARY OF THE THESIS

SUBMITTED

FOR THE DEGREE OF Ph.D. IN LAW

"GLOBAL COBWEB: CYBER CRIMES IN THE BORDERLESS WORLD: A COMPARATIVE PERSPECTIVE WITH SPECIAL REFERENCE TO U.S.A., CANADA AND INDIA"

SUBMITTED BY

Mr. GHANSHYAM SOLANKI

DEPARTMENT OF LAW

FACULTY OF LAW

THE M.S. UNIVERSITY OF BARODA

VADODARA

Dr. SYED MASWOOD
I/C HEAD AND DEAN
DEPARTMENT OF LAW
FACULTY OF LAW
THE M.S. UNIVERSITY OF BARODA
VADODARA

PROF. Dr. S.N. PARIKH
GUIDE
DEPARTMENT OF LAW
FACULTY OF LAW
THE M.S. UNIVERSITY OF BARODA
VADODARA

INTRODUCTION

The subject matter of any legal studies is pertaining to law. In as much as, law, in some form or other has existed since human beings first associated themselves in settled communities, it is clear that there has been continuous examination of the nature and function law. From the beginning of the civilization there has existed some mode of communication. As the civilization developed these modes of communication also changed. A human being always strives for better comfort or convenience and inventing and adopting new modes of communications is no exception to it.

Such a process is an elementary founding stone to the practice of law at any rate in a developed society. Thus as the civilization developed, man has constantly adapted himself with the changing circumstances and scenarios to usher in new eras of development and progress. Every stage of human history has been important in its own way. However, if today we think in retrospect and try to analyze the pace of various important advances, some periods stand out...

As the civilization enters into the new millennium, technology has suddenly taken a new meaning. The world is undergoing a technological revolution. This revolution has created new complex legal problems, over which no government is able to exercise complete control. As the human civilization develops new questions and problems crop-up. In welfare state it is never expected that law should be static. It has to change with the change and development of the society. But this change is not an overnight process. It is a gradual process of metamorphosis, and law must keep pace with these changing needs of the society. Law must respond to the cry of the

community and it must be ready to serve the needs of the society. New problems ask for new solutions and to resolve such problems law must be flexible enough. Old, rigid and outdated laws have no place in developing societies.

With the advent of "INTERNET" the world has become a global village, whereby present law enforcement machinery may not be adequate to satisfy the needs. The Internet had its beginnings in the late 1940s at the US Department of Defense during Cold War where the main aim was to maintain communications in the event of nuclear attack. The Department of Defense established the Advanced Research Projects Agency (ARPA), which created ARPAnet, the embryonic Internet. ARPAnet was used to connect vital US military and research sites. Because the computers at these sites were of different types, ARPA developed a common language, or protocol, that enabled secure communication among them. In the late 1980s, the National Science Foundation (NSF) began expanding its own network, NSFnet, with the goal of allowing access to educational and national research institutions for exchange of e-mail, files and data. Based on ARPAnet technology and protocols, NSFnet evolved to connect with other TCP/IP networks around the world, to allow open, public participation, and to be called Internet. Commercial use of the Internet began to grow slowly in the early 1990s and then virtually exploded as corporations came to realize the Internet's value for promotions, public relations, information dissemination, and the beginnings of electronic commerce. Information sent via net is broken into bites and these bites will select its own route to reach the destination. Finally they will get together at the destination. Thus net is decentralized..i.e. no human agency regulates the way the information travels.

In the last decade the human civilization has witnessed a significant technological transformation. It is felt that law must have a universal quality in the present era in its application. The explosion of new and pertinent statutory laws over the past two decades reflect society's attempt to wrestle with an ancient phenomenon in a modern context. Wrongs of all sorts occur all the times, and the individuals, organizations and legal machinery try to address them in all possible ways.

The dawn of the new millennium has given us a new mode of communication. The information superhighway is undergoing a rapid growth. The Internet and other telecommunication technologies are promoting advances in virtually every aspects of society and every corner of the globe fostering commerce, improving education and health care, promoting participatory democracy in Indian and other countries, and facilitating communications among family, friends, whether across the streets or around the world. The Internet is re-defining the relationships and transforming the lives in such a way that the communication will never be the same again. With the Internet, one can communicate at the click of the mouse to the nook and corner of the world. Immediacies and interactivity are the key words of Internet revolution.

Unfortunately, many of the attributes of modern technology such as low cost, ease of use, and anonymous nature, etc.- make it an attractive medium for fraudulent scams, child sexual exploitation, website hacking, introducing viruses, and so on. Conventional law, which provides dispute resolution machinery, fails in this 'CYBER JUNGLE'. Internet is re-wiring our relationships and the life is never

going to be the same again. This advent of global computer network has rendered geographic boundaries increasingly porous and ephemeral. As digital technology has advanced over the past 50 odd years with a force unprecedented in history, governments, business and people around the world have been affected immeasurably. The already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary data changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of earlier generations...

It goes without saying that the aforesaid new technological developments have conferred substantial benefits. However, fundamental restructuring of society also results in certain disadvantages at all levels. Our vulnerability increases with the perceived value of and reliance on this technology. Increased opportunities for the industrious to be more productive also allow the less-upright avenues for malevolence...Internet which is the cheapest and the fastest mode of communication has brought with it a new name of crime, called cyber crime. In the information age the rapid development of computers, telecommunications and other technologies have led to the evolution of new forms of trans-national crimes known as "cyber crimes". Cyber crimes have virtually no boundaries and may affect every country in the world. They may be defined as "any crime with the help of computer and telecommunication technology", with the purpose of influencing the functioning of computer or the computer systems.

Laws develop in response to society's needs. They evolve in the context of the culture, business practices and contemporary

technologies. The law currently governing commercial transactions were largely developed at a time when telegraphs and typewriters were commonly used, office technologies and business was conducted with paper documents and through mail. Technologies and business practices have dramatically changed but the law has been slower to adopt. Computers, electronic networks and information systems are now used to process, store and transmit digital data in commercial field. As the spread and use of information technologies in the business world have quickened, inadequacies and deficiencies of the current laws to meet the needs of digital, information-based society have become apparent. Electronic commerce has opened a new way of doing business. A variety of new challenges have come up for those who use Internet for business purposes.

A new stream of law – Cyber law - has emerged. Cyber law refers to the legal issues that arise within the newly emerging area that is increasingly becoming known as cyberspace. More specifically, it relates to the interaction of law with information communications technologies and computer mediated communications systems. It, therefore, has a different agenda to that of either computer law or the law of the Internet, which, respectively, often show little difference from the law relating to contract or patents, or publishing or broadcasting law. Cyber law nevertheless has a separate identity. The distinctions among the three relate not just to subject areas but, importantly, to the qualitatively different levels with which each engage with the study of law. Cyber law exists at the (cutting) edge of law, where the ability of existing law to achieve its goals is challenged. In this sense the "law" in Cyber law is a much broader concept, it is "law in action" as opposed to "law in books" as it applies to situations

where Law cannot cope. It therefore takes as its subject the wider range of regulatory responses and strategies of governance that subsequently arise. Activities in cyberspace have influenced many branches of law, like Commercial law, Intellectual Property law, and Evidence law. Unique situations, created by the tremendous growth of the Internet usage, have to be addressed in Cyber law. While legal systems of different countries are grappling with the questions of developing Cyber law by applying law or through innovations designed to meet the novel challenges (especially problem of jurisdiction) posed by the Internet, time alone can tell whether the progress will be adequate to meet the evolving business needs of the global community.... It remains to be seen whether the current approaches to deter and redress computer crime will prove successful. Naturally, Case law has been slow to develop. Most likely, it is still in a nascent wave of inevitable prosecutions. All elements of law enforcement are themselves – by and large – in infant stage.

SIGNIFICANCE OF THE STUDY

Much has been said about the coming of the Internet and how it contributes to and detracts from our lives. A prime concern as we stand on the threshold of life in the Internet age is the role it will play in the perpetration of crime.

The Internet, together with other telecommunications wonders, has turned the world into a global village. It has eased and expedited the pace of communication and interaction among business communities, consumers, government agencies and society in general by removing traditional middlemen links and cutting through unnecessary red tape. This enhances overall efficiency and results in increased productivity in

all sectors of the economy. The technology that has spurred the growth of the Internet is still changing at an expedient rate and the traditional paradigm that the world is used to in managing its affairs has been changed irreversibly. Unfortunately, like all previous inventions of mankind, Internet technology can be used for both good and evil purposes. In the wrong hands, it will facilitate the commission of all traditional criminal activities and spawn a whole new series of criminal activities called cybercrimes, which the world may be ill equipped to cope with, if the problem is not nipped in the bud. Society is facing a new name of crime called cyber crime. A name, which was unheard, has now become a part of our lives.

The significance of the study lies in the fact that Internet, which is decentralised mode of communication has given birth to the new form of crime called cyber crime. The researcher via his work tries analyze what kind of jurisdiction problems the courts have to face while resolving disputes relating to cyber crimes. Society is facing crimes like Hacking, Launching virus, Password sniffing, Cyber stalking, Internet gambling, Spamming, Software piracy etc. What has become a worst nightmare is the then law enforcing machinery fails in this cyber jungle. The moot question that has troubled almost all the nations is – 'which court has jurisdiction to resolve Internet disputes'. Use of Cyberspace is a unique and entirely new means of mass communications that is located in no specific geographical location and yet is accessible to anyone, anywhere, who has availability to it through computer link to the Internet. Consequently, there is no single organization or nation that controls membership in this virtual land, nor is there a centralized location from which access is regulated. These features of Internet make it different from other means of

communication.. The decentralized nature of the Internet poses challenging problems for the terrestrially bound government and individuals that have an interest in the real injury generated through the use of this "unregulated" medium. Since no single government controls the citizenship of Cyberspace it opens up a green ground for criminals for committing conventional crimes (also cyber crimes) via new mode of technology. Jurisdiction is the power of the court to decide the disputes between the parties. Without jurisdiction, the judgment of the court would be of no value. Internet has vanished the geographical boundaries, which use to play significant role in deciding disputes. On-line transaction has given rise to novel question of 'Jurisdiction'. The Internet permits netizen to interact and transact with one another across geographical boundaries with luxurious ease.

The researcher in this work has attempted to answer these burning issues as to which court has a jurisdiction to resolve the disputes when there is crime via Internet. It is found that Conventional law enforcement machinery is not applicable becoze Internet has no geographical boundaries. The question that arises is which court has a jurisdiction to resolve the dispute when there arises a conflict of law situation. It is quite obvious that when there will be cross-border transaction there are bound to be conflicts of law situations. The situation becomes more difficult when the transactions are done through Internet, which doesn't respect nations boundaries. Attempts are made at both national and international levels to answer these questions. The ability of the Internet to reach across borders has raised a host of questions, including questions of legal jurisdiction. Should defendants be haled to a jurisdiction where, though their websites are accessible, they had no intent to do business? Several

recent court decisions on interstate jurisdiction point to the beginnings of a standard for determining whether an entity has "purposefully" directed itself to Internet users in another jurisdiction. At the international level, the disparate legal approaches between countries magnify the potential problems. The Internet has created many challenging legal issues for the courts, not the least of which is the question of jurisdiction (the power to hear a case). The Internet can allow computer users anywhere in the world to search and retrieve information from a publicly available site anywhere else in the world. Although this potential global audience can mean great exposure for businesses, it can also translate into potential liability.

The significance of the research work lies in the fact that this study tries to focus on the most burning problem of the world as on today's date. The study focuses on problems like which courts have jurisdiction to resolve on-line disputes involving conflict of law situation. Further the work focuses on the question as to how cyber crime is different from conventional crimes. Also in-depth analysis is made as to how Internet works and what makes it decentralized mode of communication. The researcher has made a critical study of the IT Act and also focused on some of the lacunas in the Act. A comparative study of jurisdictional principles of the U.S. and Canadian law is also done. Extensive study of the case laws has been made. The decisions given by US courts have been analyzed from Indian perspective. Study is also done in the cases where the courts have given divergent opinions though the facts of the cases were similar. After going through the laws of the USA and Canada a comparative study is done with IT Act 2000. Also in depth analyze of the recent Internet related case laws has been done.

OBJECTIVE OF THE STUDY

Cross border transactions are becoming common and therefore Internet contracts have given rise to conflicts of law situation. Different countries are having different laws and therefore at times it becomes difficult to tackle the disputed problems.

The study centers round the problem of jurisdiction, which the disputing parties have to face when they had cross-border transaction via Internet. Conventional law works on the premise of geographical boundaries, which is not applicable to Internet. What exactly are 'cybercrimes'? In loose terms, they refer to any criminal activities that are facilitated by or committed by the use of or against a computer. Under this broad definition, cybercrimes are viewed as a sub-set or an extension of the generic term 'crime' and anybody who uses a computer has the potential to become a cyber criminal. For example, a traditional criminal, such as an unlicensed gambling racketeer, may be re-classified as a cyber criminal if he sets up websites offering online gambling in addition to his gambling dens. However, the criminal laws outlawing gambling will apply across the board, irrespective of the virtual mode of operation for the purposes of imposing criminal liability.

Some believe that cybercrimes is a separate and distinct phenomenon from traditional crime with material differences that require a new approach in the imposition of criminal liability. Underlying this belief is the perception that virtual crimes are actions in cyberspace, i.e. a shared virtual community that is fundamentally different from crimes committed in the physical world. As such, the application and

standards of criminal laws for the virtual community should be markedly different from those commonly applied in the courts of the physical world. Though appearing far-fetched at this point in time, the consequences of adopting this view are that it will result in the creation of cyber courts administering, perhaps, cyber justice.

Be that as it may, the harm suffered by individuals or corporations arising from cybercrimes are real and can be proven in court. Often, cybercrimes extend beyond national borders and involve the laws and people of different nations. This makes their detection all the more tedious, especially when investigative agencies of the respective countries are not co-ordinated in their field operations and are caught in a quagmire of multiple jurisdictional and conflict of laws issues. Accordingly, it is imperative that our laws and enforcement agencies keep up with technological development and form international alliances to curb this global menace.

<u>The object of the study is to focus on following issues:</u>

- Whose jurisdiction is there in cyberspace?
- Which nations laws are to be applicable when there arises conflicts of law situation?
- What are the problems that the law enforcement machinery has to face while enforcing the principles of jurisdiction?
- Can we apply the old rules of jurisdiction to Internet?
- A study of provisions relating to jurisdiction in Information Technology Act 2000.
- Comparison of basis of jurisdiction in the USA and Canada with IT Act 2000 with detail study of case law.

- To recommend necessary amendments in IT Act 2000
- To study various approaches that has been adopted by the USA, Canada and India to regulate Internet.
- Various Cyber crimes and legal provisions to curb the same

HYPOTHESIS FORMULATED

Since cybercrimes cross multiple jurisdictions, the obvious difficulty in any legislation enacted to regulate conduct in cyberspace is empowering domestic courts with the right to hear cases on crimes committed in foreign countries and involving international personalities. For example, the state prosecutor of a country will have to consider the issue of whether foreign operators of a website situated in cyberspace or in another country that offers online illegal activities, such as gambling and pornography, may be prosecuted in the former country that outlawed gambling and pornography. This is important when these foreign operators target members of the prosecuting country as the consumers of the services offered by their websites. A negative answer will impair the ability of the prosecuting state to control or regulate the prohibited activities in its own country. This is because the perpetrators of such activities could avoid criminal liability simply by operating their website out of jurisdiction. More complications arise when the laws in the countries in which these foreign operators operate from recognise the online activities as legal, e.g. online gambling and adult sites may well be legal in certain states in the US and Australia. The issue then is the status of the actions of such individuals as far as the laws of those countries, which outlawed those activities, are concerned. Can these persons be arrested for

having committed an offence in the other countries when they step foot there? Likewise, can operators of certain websites in Singapore containing politically or religiously sensitive materials be incarcerated in neighboring countries where such sites are outlawed, assuming their cyber laws have extraterritorial effect? Whatever the answer may be, one thing is certain: steps will have to be taken to evolve universally accepted laws to govern cyberspace in order to avoid an absurd situation whereby the legality of virtual acts are determined by the location of commission, which would be totally inconsistent with the borderless realm of cyberspace.

Apart from jurisdictional difficulties, the enforcement of cyber laws are equally, if not more, problematic. Enforcement agencies, which do not have adequate technical knowledge, will be hampered in their attempt to complete the evidentiary link between cybercrimes and the cyber criminal. More sophisticated cybercriminals will be able to erase all evidence of wrong doings or make their detection impossible by logging into websites under the cloak of anonymity or by impersonating somebody else or by simply rerouting their logged on paths through a convoluted web of servers circulating through several countries before hitting the computers of their victims, who may be their colleagues sitting at the next table. The improbability of the detection of cybercrimes is a very serious problem because it attacks the very pillars on which the Rule of Law stands. If the perpetrator of a cybercrime can go undetected on the basis of his superior technological knowledge, then the law will lose its bite and there will be anarchy in cyberspace. By reason thereof, some have argued for the proposition that the relevant authorities must be given the technological edge in dealing with cybercriminals, including the leeway

to 'tap' or secretly hack into the computers of suspected cybercriminals in the same manner that telephone lines of suspected criminals are monitored, in aiding the policing of cyberspace for the larger interest and the common good of the virtual community.
Some important hypothesis has been formulated to conduct the study.

They are as follows:

- Internet, which is the latest mode of communication, does not consider geographical boundaries. Cross border transactions between the parties via Internet has given rise to a novel problem of jurisdiction and conflict of law situation.
- Internet is decentralized media and it is not possible to regulate the contents available through it.
- Different nations are having different laws and therefore it becomes more difficult to regulate the net. Moreover there is also a difference in the moral standards among the nations which gives rise to hurdles to regulate the net.
- Basis of jurisdictions are vague in some nations and therefore there is no consistency in the jurisdictional principles.
- Law enforcement becomes more difficult as Internet is decentralized mode of communication. Conventional law enforcement machinery fails in this cyber jungle.
- Legislations enacted to answer the jurisdictional problem are very general in form. At times they fail to answer specific problems like IPR theft, Cyber stalking etc.

METHODOLOGY ADOPTED

As the duty is both technological and legal in nature, it is not possible to study these aspects by experimental method and hence Doctrinal Method is adopted for the study.

To conduct the study, the relevant information is collected from the specific and related enactments, various rules prescribed by both private and governmental agencies and related conventions and treaties at the National and International level. The study also deals with various Rules and Doctrines evolved by the judiciary in specific cases.

The area of law is still in its initial and developing stage and therefore it is required to rely heavily on the primary and secondary sources from which the relevant material is collected to conduct the study. The material and information are collected from sources like various relevant statutes, published books, published works, National and International journals, paper presented at National and International seminars, symposia, conference and workshops, original judgments of various National and International courts and relevant web-sites available on the topic. The study also includes a comparative analysis made of various national and international legislations on the subject. An effort has been made to compare and contrast the analysis drawn from the views expressed by such agencies that are at the helm of affairs.

REVIEW OF THE CHAPTERS

The study reviews the complexities and uncertainties surrounding the impact of jurisdictional aspects of cyber crime. Keeping this in view the researcher has divided the study on seven chapters dealing with different dimensions of the problem.

First chapter - Historically, law evolved by way of social customs, which was accepted by the society even before the legislation came into force. Voluntary forms of governance through customary private laws pre-existed state law and effectively ordered human affairs. Law arose as a spontaneous order – something to be discovered rather than enacted. Law is an evolutionary systemic process involving the experiences of a large number of people. With the advent of the Advance Technology and Globalization the fundamental concepts of Law are required to be changed. It is now felt that rapid growth is in need of swift responses. Explosion in the Information Technology has paved a way to 'INTERNET'. Conventional law machinery has failed to combat the new forms of crimes called Cyber crimes. Internet is re-wiring our relationships and the life is never going to be the same again. . A new stream of law – Cyber law has emerged. The beauty if the Internet is that, it breaks the data into bytes and these bytes will take up their own route to reach to the destination. The Internet is a rare example of a true, modern, functional anarchy. There is no "Internet Inc." There are no official censors, no bosses, no board of directors, and no stockholders. In principle, any node can speak as a peer to any other node, as long as it obeys the rules of the TCP/IP protocols, which are strictly technical, not social or political. First-time Internet users are often surprised by how hard it can be just to set up

a computer with Internet access. Why isn't it as simple as hooking up cable TV or a telephone? Once online, new users are also surprised - and often frustrated - by the lack of organization or clear authority. "Isn't anyone in charge here?" they wonder. "Who runs the Net?" The truth is that no one runs the Internet. At least not the way that government rigidly control telephone, TV, and postal service in India. The Internet works, not because of strong-armed authority, but because of cooperation and conformance to technical standards.

Chapter two - Legal Regulation of Cyberspace is, perhaps, the most challenging task of the legal machinery of any particular country. The reason is not too far to seek. The legal regime operating in the physical territory of any particular nation is too inadequate to regulate this space. If the problem is at a global level, the solution also has to be of a matching proportion. The global body namely, UNCITRAL (United Nations Commission on International Trade Law) rose to the occasion and has drafted the model law which bolsters international contracts through electronic medium. This model law is known as UNCITRAL Model Law on Electronic Commerce, 1996. The General Assembly of the United Nations by resolution dated the 30th January, 1997 adopted the Model Law on Electronic Commerce and recommended that all States should give favorable consideration to the Model Law when they enact or revise their laws. Till 1999, India didn't have legislation, to govern Cyberspace. The Department of Electronics (DoE) in July 1998 drafted the bill. The Union Cabinet approved the bill on May 13, 2000 and both the houses of Parliament finally passed it by May 17, 2000. The Presidential Assent was finally received in the third week of June 2000. The Act came into effect on 17.10.2000. Following are the objectives of the Act:

- Data, electronic forms and electronic records get legal recognition. They are now admissible in evidence just like paper-based documents.
- The Act gives legal recognition to the system of digital signatures. Digital signature performs the duty of a regular signature. Government will prescribe rules for affixing digital signature.
- Applications and documents can be filed with Government in electronic form.

The Act consists if 94 Sections. Various amendments have been made in The Indian Penal Code, Indian Evidence Act, Bankers Books of Evidence Act, and Reserve Bank of India Act. The Act though does not define 'cyber crime', it does discuss on certain specific kinds of cyber crimes like Hacking, Launching of Virus, Cyber Pornography etc. It Act contains various provisions on Penalty and imprisonment for different kinds of cyber crimes. The Act provides for the appointments of Adjudicating officers by Central Government not below the rank of Director to the Government of India or equivalent officer of the State Government as an adjudicating officer to adjudicate upon any inquiry in connection with the contravention of the Act. The also further provides for creation of A Cyber Regulations Appellate Tribunal (CRAT) for appeals from the order of any adjudicating officer. Lastly the researcher has drawn attention on certain loopholes of the Act. An attempt is also made to make certain well-built suggestions to deal with the lacunas of the Act.

Chapter three - Cyber crime is probably the most commonly used terminologies of the modern era. The birth of Internet and its rapid growth has led to the evolution of new forms of trans-national crime known as "cyber crimes". The Internet and its unprecedented rapid

growth, has raised many challenges not only for the governments but also for trade and commerce and individuals around the world. It is unfortunate that Internet has its darker side too. Many of the characteristic features of Internet like, low cost, easy to use and fastest means of communication also gives rise to new forms of crimes like fraudulent scams, child pornography, hacking, and introducing viruses. Conventional law, which provides dispute resolution machinery, fails in this cyber world. we may define cyber crime as, "A criminal offense that has been created or made possible by the advent of computer technology, or a traditional crime which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime." Even the Information Technology Act 2000, which deals with certain offences relating to Internet, does not define cyber crime. Hacking, Launching of Virus, Cyber pornography, Cyber Stalking, Cyber Defamation, E-mail Spoofing etc are some of the instances of cyber crimes. The Information Technology Act 2000 has relevant provisions to deal with these new types of crimes. Apart from the IT Act, wherever the IT Act is silent (for e.g. on cyber defamation, cyber stalking, cyber gambling) relevant provisions of the Indian Penal Code and also principles of Law of Torts will be applicable. The researcher has discussed the provisions of the IPC or principles of Law of Torts could be applicable where the IT Act is silent.

Chapter four - Unfortunately, the Internet is not all flowers and sunshine. There are elements within it that have grown to become sources of anxiety within our society. Among them is the pervasive availability of Pornography or more commonly known Cyberporn.

Cyberporn has become the most controversial topic arising from the use of the Internet in recent years. Free availability of pornography on the Internet has gained the attention of law enforcement bodies. Starting form the historical aspect of pornography to Internet, the researcher has covered the relevant provisions of the IT Act and IPC to curb the evil of pornography. Also relevant provision of Indecent Representation of Women's (Prohibition) Act 1986 is covered. There is also a comparative study on how the US and Canadian law enforcement machinery is trying to grapple with this menace. The study also covers certain basic difference on 'obscenity' and 'pornography'. An attempt is made to find as to how cyber pornography is difficult to regulate. Lastly the study covers certain suggestions to curb the menace of cyber porn.

Chapter five is the core part of the research work. It exclusively deals with the issue of Jurisdiction, its evolution, and kinds. Initially it starts with the basis of civil and criminal jurisdiction of Indian courts. Then it deals with the question whether these principles of jurisdiction applies to Internet. It also discusses in detail the pros and cons of jurisdiction provisions in the IT Act. The chapter goes further to discuss in detail the jurisdictional provisions of USA and Canada and comparative study is made. E-commerce has become the buzzword of the world. The zest of doing global transactions through Internet has become irresistible. Ironically, because a page on the World Wide Web can reach web surfers in every corner of the world, there arises the issue where exactly a person who has a cause of action, based upon a web transaction, may sue. The unique characteristics of the Internet such as its decentralised nature, disregard of territorial based boundaries,

low cost, and fastest mode of communication may easily give rise to issues that involve parties from more than one jurisdiction. Detail study on history of evolution of principles of Jurisdiction in the USA. The study covers almost all the relevant case laws from pre-Internet era to post-Internet era. Detail study of Indian law of Jurisdiction is also a core part of the subject. An attempt is made to justify the topic to the maximum. Comparative study on the US and Indian law of jurisdiction is made.

Chapter six - Privacy is a fundamental human right. It protects human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age. Privacy is recognized around the world in different regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. With the growth and development of new technological advancements, society and government also recognized its importance. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. Protection of privacy is one of the critical issues that must be resolved. Will the "Digital Age" be one in which individuals maintain, lose, or gain control over information about themselves? Will it be possible to preserve a protected sphere from unreasonable government and private sector intrusion? In the midst of this uncertainty, there are reasons for optimism. Individuals give their personal information regarding their financial status to the Banks, patients give their personal information regarding the ailments from which they suffer to the doctors, individuals also give their personal

information to the insurance company while taking insurance. Further while subscribing for the new credit card one had to give his personal information. All this information, which was earlier, noted down on the papers, now stored in the hard drive of doctor, insurance company, or credit card company's computers. There are very fair chances that if this information is passed on to somebody else which an individual is not aware about, it would surely amount to breach of right of privacy. The study covers various provisions of the law to deal with the violation of the right to privacy. Also a comparative study is made between the US, Indian and Canadian laws to deal with the issue. Lastly, the study focuses on certain specific measures that could be taken to deal with the violation of the right of privacy.

Chapter seven - The Internet has given rise to number of legal questions. If a defamatory statement is placed on a website, it is accessible to millions of users simultaneously. How can we track down the culprit, and where should we bring him to justice? In a space where physical boundaries do not mean anything, how shall we determine jurisdiction? If a hacker hacks into a computer system half way across the world, which legal system should we use to convict him? How would extradition work in such a situation? The chapter discusses in details various modes for combating cyber crimes. In depth study is made on topic like installing filtering software's, signing of multilateral treaties, and creation of International Organization to deal with the issue. In-depth study is made on various legislations that have been enacted by the US and Indian law enforcement mechanism. Lastly there is critical study of the various modes for curbing cyber crimes.

Chapter eight - The Internet is probably the largest of the open networks, which now form a diffuse global entity. The notion of physical territory is necessarily alien to the technical norms governing the Internet--instead, the standards and protocols of Internet communication have developed in such a way as to transcend 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 found 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 government has failed to regulate the Internet to its fullest extent. 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, it is quite impossible to effectively regulate. The study ends with certain important suggestions so as to deal with cyber crimes.