Chapter 1

THE WORLD OF CYBERSPACE

"The ability of the World Wide Web (Internet) to penetrate every home and community across the globe has both positive and negative implications- while it can be an invaluable source of information and means of communication, it can also override community values and standards, subjecting them to whatever more may or may not be found online….The Internet is a challenge to the sovereignty of civilized communities, States, and nations to decide what is appropriate and decent behaviour."

Statement of Rep.Goodlatte in US Congress[1]

1.1 Introduction

Three times in the past 250 years the world has witnessed a major transformation affecting virtually every aspect of society. Founded on advances in science and fueled by innovations in technology, these industrial revolutions produced major leaps forward in human productivity and changed the way people work and interact with each other. By the time such a revolution runs its course, virtually every aspect of society has been affected in some significant way[2].

The first industrial revolution originated in Britain and lasted from roughly 1760 to 1830. It was founded on new methods of manufacturing based on iron and steam, and at its core were the first major advances since antiquity to use scientific reasoning to develop new products - in short, modern applied research[3]. These innovations ultimately spurred new forms of transportation such as the steamship

[1] Rep.Goodlatte is a member of House Judiciary Committee in US. This committee frequently weighs in on policy issues destined for implementation by the Federal Communication Commission (FCC).
[2] Bradford L. Smith, The Third Industrial Revolution: Policymaking for the Internet, 3 COLUM. SCI. & TECH. L. REV. 1, (Nov. 4, 2001) available at http://www.stlr.org/cite.cgi?volume=3&article=1 , visited on 14 Nov 2003.
[3] ibid

and the railroad, as well as the invention of mechanical looms and other machinery, which together prompted socio-economic changes such as the introduction of specialized labor and the factory system[4].Specialization and factories, in turn, led to widespread population shifts from rural to urban areas and to fundamental changes in the way people worked and interacted.

The second industrial revolution lasted from about 1875 to 1930. It was powered by inventions such as electricity, the telephone and the internal combustion engine and automobile, as well as new synthetics and alloys and new applications of steel and oil. These advances were made possible by the unprecedented availability of capital and the creation of the modern business organization. Among the revolution's many socio-economic effects were greater mobility, a growing middle class and the beginnings of more widespread leisure time[5].

Although different in many ways, these industrial revolutions shared certain characteristics. First, each was founded upon one or more new technologies that fundamentally changed manufacturing processes in a number of industries. Second, the adoption of these new technologies made it possible for manufacturers to improve productivity, which ultimately resulted in greater purchasing power and higher standards of living for broad segments of the population. Finally, these new technologies exerted profound and lasting effects on how people worked, socialized and used their leisure time.

Today the Internet is at the heart of a third industrial revolution. Made possible by technological advances in computer hardware, software, and telecommunications, the Internet has forced companies everywhere to reinvent themselves and the way they do business. This transformation in business practices has fueled unprecedented gains in productivity, generated both by improvements in efficiency and the creation of new markets. At the same time, the Internet is profoundly

[4] ibid
[5] ibid

changing the way people communicate with one another and express and enjoy themselves.

But as in any period of dramatic change, the Internet revolution raises several challenges and questions for legal systems around the world. To what extent do we need to adapt existing legal structures to facilitate efficient commercial practices while promoting innovation? How do we ensure that the law advances important social values that transcend these commercial interests? More fundamentally, what are the appropriate responsibilities of the public and private sectors in addressing these issues? Although several legal scholars -including David Post, James Boyle, Lawrence Lessig and others have offered insightful critiques of law's relationship to the Internet, these authors have been less successful in articulating a coherent model for resolving the many social and legal issues that arise online.

1.2 Law and Technology

Human history in a sense is a story of technology from flint stones to that of genetic. The tribulations and triumph of such a journey which will continue in the future, has one aspect, constant at its core – "the laws that govern them". Technology- if defined as 'set of refined processes' resulting in various application of daily use in our lives seems to be harmless marvel in its basic construct and explanation.

Technology has been an instrument of social change. Before the invention of automobiles there was no need for traffic signal lights and policemen and law to regulate the automobiles. Copyright law was created in the late Middle Ages in reaction to the invention and use of printing press. Similarly only after the invention of ship, maritime law developed. New technologies are human inventions. Technologies are a product of ingenious creativity forced by ecological, social or cultural pressures such as capitalist systems, economic pressures to increase productivity or political and military pressures such as warfare or ecological and demographic threats to a given society[6]. Technology, law, economic conditions and

[6] Lessig, Lawrence, Future of Ideas, The Penguin Press, New York, 2005

practices, social relations and cultural conceptions are different systems or contexts within which human beings act, alone and with others[7].

The rapid advances in science and medicine since 1950, and especially the advances in computer technology since 1980, have revolutionized the way society functions. It is widely recognized that our society is making a transition from the industrial manufacturing age to an information age. In contrast, law is struggling to keep pace with the technological advancements which are causing social changes in leaps and bounds[8].

Law has been slow to adapt to the choices posed by technology. It is accepted fact that knowledge, opportunities, and choices are inherently good, there are the possibilities of (i) prohibiting or restricting use of new technologies for no good reason or (ii) of misusing technology to harm people. Law that made sense in 1850, or even in 1950, can be inappropriate for today's problems and opportunities[9].

One of the important reasons why law takes its own time to adjust to new ideas and slow to change is that the evolved judicial principles. One of the basic principles of jurisprudence is *stare decisis*: the old decision stands as a precedent for the present and future. Such a principle gives society stable law, so that attorneys can predict the outcome of a case and advise their client. Therefore, judges are reluctant to make new law[10].

---

[7] Benklar Yochai, Technology, law Freedom and Development, The Indian Journal of Law and Technology , Vol.1, 2005

[8] Standler B Ronald, Response of Law to New Technology, available at http://www.rbs2.com/lt.htm, visited on 1 Jan 2004

[9] ibid

[10] ibid

Technology does not determine society, it embodies it. But nor does society determine technological innovations, it uses it. This dialectical interaction between society and technology has become part of the living society[11].

1.3 The Advent of Internet

The 'space race' has been identified as a catalyst for the development of personal computers, the argument being that the US had to minimize the size and weight of on board computers in order to compensate for the greater power of soviet rockets. The connection between the space race and the Internet is less well known, but may be equally significant[12].

The first artificial satellite, SPUTNIK, was launched in 1957 to great consternation in the US defense establishment. As part of its response, the Advanced Research Projects Agency (ARPA) was established under the auspices of the department of defense, with a remit of establishing US leadership in areas of science and technology which might posses military applications.[13]

The concept of a decentralized computer network had been considered in a number of countries, including the UK, but it was with the provision of substantial funding from ARPA in 1964 that a practical implementation was developed. The project was based upon ideas drawn up by Paul Baran of the RAND Corporation, an organization described as 'America's foremost cold war think tank. Its genesis lay in the desire to find a method of enabling the US military and government to maintain communications after a nuclear war. The assumption was that telecommunication control centers would be leading target for attack and that traditional telecommunications networks would be rendered unusable. The solution lay in reversing the conception that a telecommunications network should seek to be as reliable as possible by building in the assumption of unreliability. From this starting point, the system should be designed in such a way as to enable messages

[11] Castells, Manuel, The Rise of Network Society, 2nd Edition, Blackwell Publishing Ltd., New York, 2002

[12] Lloyd J Ian, Information Technology Law,3rd edition, Butterworths, London,2000, at p 17

[13] ibid at p 17

to overcome obstacles. The system would link a number of computers or 'nodes'. Every message would be sent on their way and would pass from node to node until all arrived at the intended destination, where they would be reassembled to indicate the complete message. Although packets would be forwarded in approximately the correct direction the particular route taken by a packet would be dependent upon chance and network availability. If one section of the network had been damaged, the packets would be routed via other sections. A helpful illustration might be to analogize the system with the road network for transportation. The motorway network might be compared with a telecommunications network. It provides high capacity and high speed transport links. Disruption at a few key locations- by nuclear attack or less dramatic incidents- would render the system unusable. The Internet might be compared with the non- motorway road network. Travel may be slower and more circuitous, but the sheer variety of routes would make total disruption of service a most unlikely event[14] .

The initial network, ARPANET, which was named after its sponsors, was installed in 1969 with four nodes. By 1972, this figure had grown to 37. One of the next major developments was the evolution of the communication standard Transmission Control Protocol/Internet Protocol (TCP/IP). The TCP component was responsible for converting messages into streams of packets, whilst the IP is responsible for addressing and routing the packets to their destination. The TCP/IP protocols were developed in the 1970s, but it was with their adoption as the basis for ARPANET on 1st January 1983 that the Internet could be said to have originated[15].

[14] ibid at p17
[15] ibid at p18

The word 'INTERNET' has been defined in a 1995 resolution of the US federal Networking Council as follows: 'Internet[16]' refers to the global information system that

---

[16] A description of the Internet set forth by Justice John Paul Stevens in the landmark Reno v. ACLU (Eastern District Court of Pennsylvania, civil action 98-5591, available at http://supreme.usatoday.findlaw.com/supreme_court/decisions/lower_court/98-5591.html, visited on 23 Feb 2002) decision, June 26, 1997 is as follows;

The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called Advanced Research Agency Project NETwork (ARPANET), which was designed to enable computers operated by the military, defense contractors, and universities conducting defense related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."

The Internet has experienced "extraordinary growth." The number of "host" computers--those that store information and relay communications--increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e mail"),

automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium--known to its users as "cyberspace"--located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E mail enables an individual to send an electronic message--generally akin to a note or letter--to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real time dialogue--in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."

The best-known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address--%rather like a telephone number." Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text--sometimes images.

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users

(i) is logically linked together by a globally unique address space based on the internet protocol (IP)

(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and

(iii) provides, uses or makes accessible , either publicly or privately , high level services layered on the communications and related infrastructure described herein.

A feature of the TCP/IP protocols is that they enable any user to connect to the internet. These are no social or practical controls over the making of such connection and the cost implications are minimal. It is somewhat ironic that a system which was designed to enable the authorities to retain control over a nuclear wasteland should have metamorphosed into a system which is almost a byword for anarchy[17].

Cyberspace has developed with almost incredible speed, certainly when compared with other forms of communication technologies. In 1876, Alexander Graham Bell was awarded a patent for the telephone. Its impact on the world has been massive,

---

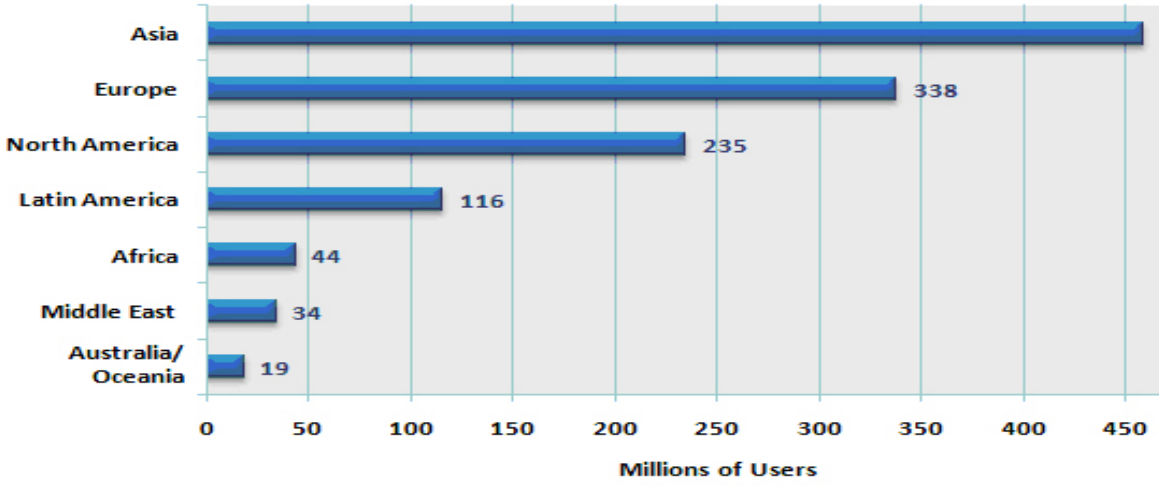
generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web."

[17] Lloyd J Ian, Information Technology Law,3rd edition, Butterworths, London,2000, at p 18

but 74 years were to elapse before 50 million subscribers were connected. Radio took 38 years to reach the same figure. With the PC, only 16 years elapsed. From its inception in 1993, WWW (World Wide Web) required only four years to acquire 50 million users. In terms of statistics in 1989, the internet had some 100,000 host computers. By 1992, this figure had climbed to 1,000,000. In 1997, the figure had increased to some 13 million sites, with the internet maintaining a 100% annual growth rate through much of the decade[18].

Internet usage statistics from a recent survey conducted by www.internetworldstat.com is depicted below by a graph;



For users in the developed world, the internet is becoming a feature of our everyday lives. It is rare to find a newspaper which does not contain some feature on the internet. Most newspapers, and many television and radio programmes, maintain an electronic presence on the internet. Many advertisements and publicity documents refer readers to an internet site for further information[19].

The internet and the WWW are but one manifestation of a radical change in the nature of society which has been brought about by the computer. It is now a trite

[18] ibid
[19] See generally, Developments in the Law- The Law of Cyberspace, Harvard Law Review, Vol.112:1574, The Harvard Law Review Association, 1999

comment to say that we live in an 'Information Society', in which information in its many and various forms is becoming a more important commodity and measurement of prosperity than physical objects. The question arises what is the nature of this beast and how should it be regulated?

1.3.1 Nature of Internet

Internet today is a technology used by millions of surfers connecting millions of computer worldwide. The rate of growth of this technology is quantitatively and qualitatively different than its predecessors like telephone, radio or television. Internet is a single platform where all the others can converge - information, speech and visual combined as digital information. Unlike the other technologies often referred as 'push technologies' where the process is one-way from those who produce to those who consume, internet is referred as 'push and pull technology' offering interactive process.

Nevertheless, the social behaviour of 'netiquette' of the early group of users based on mutual trust and conditioning will also change in the various stages of the history of internet. The contemporary understating of this 'free space of the commons' is often debated on themes like cyber terrorism and cyber crime making the new jurisprudence of cyber laws and the great debate of 'freedom v regulation'.

Cyberspace[20] does not exist physically, except in the countless miles of electronic circuitry, fiber optic cables and silicon chips which make up our computers and our networks. Cyberspace, by its very nature, is everywhere and nowhere at once; it is the everythingness and nothingness of William Gibson's matrix, but it need not be realized only in futuristic dystopian novel. We exist in cyberspace today, everyday. Cyberspace is where we are, in our mind's eye, when we are on the phone with a loved one across the country. Cyberspace is where we are when we watch a movie, or wear headphones. It is where an architect's computer aided design exists before it

[20] The term 'CYBERSPACE' is coined by , William Gibson, in his novel, Neuromancer, and has been extensively used to denote virtual world.

is constructed. Cyberspace is an infinite, universal space, achieved by technology inhabiting minimal amount of physical space[21].

But immersive cyberspace as mediated through virtual interfaces, unlike the infinite reaches of physical space, is nothingness. It is a blank, black void until an artificial context is introduced. It is nothing, placeless and indescribable. The void of cyberspace has no gravity and no micro or macro climate of Sun, wind, earth and water. In cyberspace even a horizon is artificial. There are no building codes, no monetary budgets and no neighbors in cyberspace[22].

Furthermore, while three dimensional space exists in cyberspace, geography does not. We exist in physical space, in a physical place, in relation to all objects around us. Above, beyond, near and far. All of these words describe ourselves and other objects in relation to a context of other specific, distinct objects. Geography, the measure of three dimensional space, exists because objects in physical space bear physical presence, separated by physical distance. Geography cannot exist in cyberspace. To overlay cyberspace with a Cartesian coordinate system is futile, for its infinite reaches collapse into nothingness. Objects, despite their three-dimensionality, do not take up space. They have no place in relationship to other objects. Any virtual object, any world, any person can exist in the same space as any other at the same time. Conversely, any virtual object, world or person can exist in an infinite number of spaces simultaneously. All information, all environments, all ideas realized spatially and electronically will be available to all persons, everywhere, at all times in cyberspace[23].

1.3.2 Internet Infrastructure for Data Transfer

The Internet, and its communication miracles, results from a fundamental principle of network engineering: Keep It Simple. Every computer connected to the Internet is capable of doing a few, very simple tasks very quickly. By linking millions of comparatively simple systems together, complex functionality is achieved. The

[21] From the series Vers Une Architecture Virtuelle, The Nature of the Cyberspace, available at http://www.hitl.washington.edu/people/dace/porfoli/crit35.html, visited on 19 Aug 2004
[22] ibid
[23] ibid

Internet is an ingenious communications network in large part because it is so simple[24].

At the heart of any Internet transmission - sending an email, viewing a web page, or downloading an audio or video file - is the Internet Protocol (IP). Invented in 1974 by Vint Cerf and Robert Kahn, IP is a communications scheme that defines how data is sent across networks. IP has two key standardized elements that are involved in every transmission: (1) a common method for breaking each transmission down into small chunks of data, known as "packets", and (2) a unified global addressing system. IP gives every computer connected to the Internet a unique address, and a common definition of the packets of data that can be delivered to these addresses[25].

In other words, the Internet Protocol boils down to two simple rules:

1. Every computer connected to the Internet must be reachable via a numerical address of a specific form: four eight-bit numbers separated by periods - e.g., A.B.C.D where A, B, C, and D are between 0-255 (that's because each eight-bit string has 2^8=256 different combinations). This address is called an "Internet Protocol address," or "IP address" for short. For example, the IP address for Google's homepage is 216.239.51.100[26].
2. Every computer connected to the Internet must be able to accept packets that have a 24 to 32 byte header and a packet size of up to 576 bytes. The header contains information on the origin[27].

Using IP, a computer first breaks down the message to be sent into small packets, each labeled with the address of the destination machine; the computer then passes those packets along to the next connected Internet machine, which looks at the

[24] Ethan Zuckerman & Andrew McLaughlin ,Introduction to Internet Architecture and Institutions , Berkman center for Internet and Society , visited on 2 May 2004, available at http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html#intro , visited on 28 Sep 2004

[25] ibid
[26] ibid
[27] ibid

destination address and then passes it along to the next connected Internet machine, which looks for the destination address and pass it along, and so forth, until the packets reach the destination machine. IP is thus a "best efforts" communication service, meaning that it does its best to deliver the sender's packets to the intended destination, but it cannot make any guarantees. If, for some reason, one of the intermediate computers "drops" (i.e., deletes) some of the packets, the dropped packets will not reach the destination and the sending computer will not know whether or why they were dropped[28].

By itself, IP can't ensure that the packets arrived in the correct order, or even that they arrived at all. That's the job of another protocol: TCP (Transmission Control Protocol). TCP sits "on top" of IP and ensures that all the packets sent from one machine to another are received and assembled in the correct order. Should any of the packets get dropped during transmission, the destination machine uses TCP to request that the sending machine resend the lost packets, and to acknowledge them when they arrive. TCP's job is to make sure that transmissions get received in full, and to notify the sender that everything arrived as sent[29].

An analogy can be drawn with the physical world to illustrate the working of TCP. Sending a communication (an email or web page or video file or whatever) via Internet Protocol packets is like sending a book by postcard. Figuratively speaking, the Internet Protocol allows your computer to take our book, cut out the pages, and glue each page onto a postcard. In order to allow the destination computer to reassemble the pages properly, your computer writes a number on each postcard, after all, there is no guarantee that the mailman will deliver the postcards in the exact right order[30].

Here's where it gets interesting. Because there's a danger that some postcards will be lost in the mail, the computer keeps a copy of each one, just in case it needs to resend a missing postcard. How will the computer know if it needs to resend some

[28] ibid
[29] ibid
[30] ibid

of the postcards? That's where TCP does its ingenious thing. TCP tells the destination computer to send a periodic confirmation postcard back to your computer, telling it that all postcards up to number X have been received. When the computer gets a confirmation postcard like that, it knows that it is safe to throw out the retained duplicate postcards up to number X. TCP also instructs the computer that, if no confirmation is received by a certain time, it should start to resend the postcards. The lack of a confirmation may mean that some postcards are missing, or that the confirmation itself got lost along the way. The computer is not too worried about sending unnecessary duplicates, because it knows that the destination computer is smart enough to recognize and ignore duplicates. In other words, TCP says that it's better to err on the side of over sending. TCP also helps computers to deal with the fact that there is a limit to how many postcards can be stuffed into a mailbox at one time. It allows the two computers to agree that the sender will only send perhaps 100 postcards and await a postcard confirming receipt of the first 100 before sending the next group[31].

Thus, TCP gives the sending and receiving computers a way to exchange information about the status of a communication, which packets have been received, which ones are missing. And it helps the two computers manage the rate of packet traffic, so as not to get overwhelmed[32].

1.3.3 Internet and Society

The Internet has revolutionized the way we live, work and communicate. It also changed the way we conduct and behave ourselves in the society. Most of the deviant conduct that may occur in cyberspace is not unknown to us or new, but the environment in which this happens is quite new and hence has to be dealt separately. Internet is a medium that remains poorly understood as result of change

[31] ibid
[32] ibid

of pace in our modern information environment and the lack of adequate supply of empirical studies of the internet[33].

All changes in systems of communication are important to the legal system and development of societies. Electronic communication has not only altered the way we communicate, it has also changed the way our societies work and are organized. The rise of the internet is a key to part of the social transformations taking place in late modernity. In order to understand this, and subsequent developments, we have to approach the internet as a modality of cultural transmission. As uncertainty about the impact of such a sophisticated communication technology undoubtedly exists, what we lack is a social theory of internet. We urgently need to find concepts and frameworks that can help us to develop a more critical understanding of the internet and continue to remain critical of what we find[34].

As far as the human rights of netizens are concerned a concrete international legal framework has to be put in place so that everyone is allowed to enjoy the benefits of this new communication medium.

1.4 Why Cyber Law?

The term cyber law has gained a wide recognition often spoke about in seminars, workshops and symposiums. Literature has been published using the terms like cyber law, Law of the Internet, Law Relating to Computers etc. In academic settings there are centers for Computer and the Law, Cyber law and research and son and so forth. The important question is whether these terms are used to denote a specific branch of study, or just a popular usage without coming to grips with what exactly is this branch of law, is it still evolving or is it a generic usage of dealing with varied existing laws on a glamorous pre-fix or suffix?

---

[33] Castells, Manuel , The Internet Galaxy-Reflections on the Internet, Business and Society, Oxford University Press, London, 2001

[34] Slevin, James, The internet and Society: Central Themes and Issues, Trojborgtrykkeriet, the Faculty of arts, University of Aarhus, The center for Internet Research, Aarhus, 2002

Judge Frank H. Easterbrook remarked at a conference on 'Law of Cyberspace', that they do not offer a course in "the Law of Horse'. He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and …" courses should be limited to subjects that could illuminate the entire field of law. And that the best way to learn the law applicable to specialized endeavors is to study the general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "the Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching hundred percent of cases on people kicked by horses will not convey the law of torts well. Far better for most students- better , even, for those who plan to go into the horse trade- to take courses in property, torts, commercial transactions, and the like , adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coals and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses[35].

Judge Easterbrook is of the clear view that developing sound laws and applying them to cyberspace to makes sense. Cyberspace requires no new laws. For example, property in cyberspace can be best examined and applied with sound and robust development of intellectual property law[36].

In contrast to the views of Judge Easterbrook, Larence Lessig argues that there is an important general point that comes from thinking in particular about how law and cyberspace connect. This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace, comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behaviour. Law in its traditional sense- an order backed by a threat directed at primary behaviour- is just one of these tools. The general point is that law can affect these other tools- that they constrain behaviour

[35] Easterbrook H Frank, Cyberspace and the Law of the Horse, 1996 U.CHI.LEGAL.F 207, available at http://www2.sims.berkeley.edu/courses/is205/s06/Readings/Easterbrook,%20Law%20of%20the%20Horse.pdf , visited on 23 June 2005

[36] ibid

themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values.

Further Lessig, highlights two important cases which illustrates the requirement of separate law for cyberspace. The first one is about difficulty in distinguishing adult from child in internet transactions and the second one is about invasion of our privacy which is quite different from the real world. Lesigg describes them as follows;

(1) Zoning Speech – Porn in real space is zoned from kids. Whether because of laws (banning the sale of porn to minors) or norms (telling us to shun those who do sell porn to minors) or the market (porn costs money), it is hard in real space for kids to buy porn; hard, but not impossible. But on balance the regulations of real space have an effect. That effect keeps kids from porn[37].

These real space regulations depend upon certain features in the design of real space. It is hard in real space to hide that you are a kid. Age in real space is a self-authenticating fact. Sure a kid may try to disguise that he is a kid; he may don a mustache or walk on stilts. But costumes are expensive and not terribly effective. And it is hard to walk on stilts. Ordinarily a kid transmits that he is kid; ordinarily, the seller of porn knows a kid is a kid, and so the seller of porn, either because of laws or norms, can at least identify underage customers. Self-authentication makes zoning in real space easy[38].

In cyberspace, age is not similarly self-authenticating. Even if the same laws and norms did apply in cyberspace and even if the constraints of the market were the same (as they are not), any effort to zone porn in cyberspace would face a very difficult problem. Age is extremely hard to certify. To a website accepting traffic, all requests are equal. There is no simple way for a website to distinguish adults from kids, and likewise, no easy way for an adult to establish that he is an adult.

---

[37] Lessig, Lawrence, The lLaw of the Horse: What Cyberlaw Might Teach, 113 HARV.L REV.501(1999), available at http://www.lessig.org/content/articles/works/finalhls.pdf , vsisted 2 Feb 2003; See also 'Code and other Laws of Cyberpsace' by Lawrence Lessig published by Basic Books, 1999 for his arguments why he suggests 'CODE' should be law.

[38] ibid

This feature of the space makes zoning speech there costly- so costly, the Supreme Court concluded in Reno V ACLU that the constitution may prohibit it[39].

(2) Protected Privacy- if you walked into a store, and the guard at the store recorded your name; if cameras tracked your every step, noting what items you looked at and what items you ignored; if any employee followed you around, calculating the time you spent in any given aisle; if before you could purchase an item you selected, the cashier demanded that you reveal who you were; if any or all of these things happened in real space, you would notice. You would notice and could then make a choice about whether you wanted to shop in such a store. Perhaps the vain enjoy the attention; perhaps the thrifty are attracted by the resulting lower prices. They might have no problem with this data collection regime. But at least you would know. Whatever the reason, whatever the consequent choice, you would know enough in real space to know to make a choice[40].

In cyberspace, you would not. You would not notice such monitoring because such tracking in cyberspace is not similarly visible. When you enter a store in cyberspace, the store can record who you are; click monitors (watching what you choose with your mouse) will track where you browse, how long you view a particular page; an employee (if only a bot) can follow you around, and when you make purchases, it can record who you are and from where you came. All this happens in cyberspace- invisibly. Data is collected but without your knowledge. Thus you cannot choose whether you will participate in or consent to this surveillance. In cyberspace, surveillance is not self-authenticating. Nothing reveals whether you are being watched, so there is no real basis upon which to consent[41].

These examples mirror each other, and present a common pattern. In each, some bit of data is missing, which means that in each, some end cannot be pursued. In the first case, that end is collective (zoning porn); in the second, it is individual (choosing privacy). But in both, it is feature of cyberspace that interferes with the particular end. And hence in both, law faces a choice- whether to regulate to change this architectural feature, or to leave cyberspace alone and disable this collective or

[39] ibid
[40] ibid
[41] ibid

individual goal. Should the law change in response to these differences? Or should the law try to change the features of cyberspace, to make them conform to the law? And if the latter, then what constraints should there be on the law's effort to change cyberspace's nature? What principles should govern the law's mucking about this space? Or again, how should law regulate?

To many these questions will seem very odd. Many believe that cyberspace simply cannot be regulated. The anonymity and multi-jurisdictionality of cyberspace makes control by government in cyberspace impossible. The nature of the space makes behaviour there unregulable[42].

This belief about cyberspace is wrong, but wrong in an interesting way. It assumes either that the nature of cyberspace is fixed- that its architecture and the control it enables cannot be changed- or that government cannot take steps to change this architecture. Neither assumption is correct. Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its design or its code. This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way and while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where beahaviour can be regulated and the government can take steps to increase this regulability[43].

There are several reasons why it is convenient to have a separate classification of law for computer and computer networks like internet:

(1) Solving legal problems that arose from the use of computers often requires some legal principles that are rarely encountered in the practice of law. For example:

(A) Disputes about e-mail and web pages on the Internet extend across state lines, and may even extend across national borders. For example, there are technical issues in personal jurisdiction and which state's law should be applied to the resolution of the dispute. To solve

[42] ibid
[43] ibid

these legal problems, one must understand principles of an abstruse area of law, called *Conflicts of Law*[44].

(B) Information stored on computers (e.g., software, data, trade secrets, confidential personal information) is generally much more valuable than the computer hardware. In order to protect this information, many of the concepts in the practice of computer law involve the specialized area of *Intellectual Property Law*, which includes copyrights, trademarks, and patents[45].

(2) Traditional concepts in law are being expanded by events in the area of computer law. For example:

(A) Computer software is legally considered a "good". Unlike other goods, the "purchaser" only owns the floppy diskette or compact disk that contains the software, plus a *license* to use the software. The Uniform Commercial Code was amended by including Article 2B to cover licensing of computer software[46].

(B) Computer databases that contain erroneous information (e.g., false credit reports) can be harmful to people, which may give rise to a new class of torts[47].

(C) Hackers who use a modem to enter a computer without authorization and either (1) use its services or (2) alter records are committing a crime similar to burglary, but the traditional notion of burglary requires the criminal personally to enter the victim's premises, which is not satisfied in the case of entry via data to/from a modem. Therefore, new laws were enacted to define computer crimes. (Personally, I think it would have been preferable to change the definitions in existing concepts, instead of create new concepts, but

---

[44] Standler B, Roland, What is Computer Law?, available at http://www.rbs2.com/cdefn.htm , visited on 1 Jan 2004
[45] ibid
[46] ibid
[47] ibid

no one would accuse the legal profession of honoring simplicity and economy.)

(D) Authentication of evidence contained in files on a computer presents some new problems, because of the ease with which data in the file can be altered, and also because it is easy to alter the operating system's date and time stamp in the directory[48].

(E) Searches of computer databases provide access to information that was difficult to locate in the pre-computer age, which makes computer databases a major new threat to privacy of individuals[49].

The Internet has been revolutionary in giving anyone with a website the equivalent of a printing press or television transmitter: now anyone can broadcast their information or opinion to the whole world, without first going through formal review by a publisher. Many governments have reacted to the Internet with new censorship of both websites and readers' access to the Internet. Furthermore, there has been widespread copyright infringement by people who post material at their website that was copied from other websites, or copied from books, without written. permission of the copyright owner. Professor Hugh Gibbons at Franklin Pierce Law Center observes

"With the exception of the telephone and typewriter, the technological revolution of the past century has left the law untouched. Law has dealt at arm's length with technology, making new rules to cover air travel, genetic engineering, and the like, while the lawyers who do the work carry on with paper and pencil – until the advent of the computer."[50]

Law grows with ad hoc additions, which are often not consistent with a small

[48] ibid
[49] ibid
[50] ibid

collection of philosophical principles, in this way law is unlike science and engineering[51].

1.5 Regulation of Cyberspace

For every country, postal and telecommunications networks have long provided an infrastructure for the transmission of information. The publishing industry has provided mass dissemination of information since Gutenberg's invention of the printing press, whilst more recently, broadcasting has performed a similar role. The novel element in the vision of a super-highway is that there should be the capability for the two-way delivery of text, pictures, sound and video. The House of Lords Select Committee on Science and Technology, in its recent report on the Information Society[52], adopted the definition of a 'publicly accessible network capable of transferring large amounts of information at high speed between users'. Although the Internet is often regarded as a major component of the information superhighway, limitations in communications technologies have led to the suggestion that it constitutes 'little more than an electronic footpath[53]'.

If consideration is given to existing forms of information transfer, a variety of actors may initially be identified:

1) Cable, terrestrial and satellite broadcasters.
2) Publishers of printed, video and audio works.
3) Telephone and telecommunication companies.
4) Software producers.
5) Internet content producers and service providers.
6) Database Producers.

The activities involved may themselves be divided into a number of categories. Broadcasting services, for example, engage in a one-way transfer of information

[51] ibid
[52] The term 'information society' has been defined as a 'society dependent on information exchanges through the use of computers and telecommunications devices'. Definition given by Niels Brugger & Henrik bodker in their paper , The Internet and Society? Questioning Answers and Answering Questions, Ppaers from The Centre for Internet Research, Aarhus, Denmark 2002
[53] Supra note 12, p16

from broadcaster to viewer or listener. The model is one of simultaneous transmission to multiple users. Although some cable networks and systems 'pay per view' constitute exceptions to the rule, the user's only interaction with the system is, generally, to decide whether or not to receive a particular transmission. The same unidirectional transfer of the supply of books, newspapers, video and audio tapes will happen, but with the distinction that the customer has much more flexibility as to the time at which the materials will be read and used. Millions of viewers will simultaneously watch the evening television news. Although millions of persons may also buy a national newspaper, the element of synchronous transfer of data is less noticeable. Telephone companies provide an infrastructure which is used by customers to exchange data. The notion of two-way transfer is also present with on-line databases and many of the aspects of the internet[54].

More significantly, the activities have been subjected to radically different regulatory schema. Although there is a general trend towards liberlisation, driven in part by developments in digital technology, sectors such as broadcasting and telecommunications have traditionally been subject to much more stringent forms of regulation than has been the case with publishers. Until the 1980s, the need for massive investment in infrastructure, coupled with political requirements to provide a universal service, meant that telecommunications tended to be the subject of a de facto or de jure monopoly. Similar factors applied to the broadcasting sector, where state control might be exerted either through the establishment of monopoly or through the operation of a system of licenses. A further significant factor was the need to ration scarce resource. The development of satellite broadcasting and the emerging system of digital television removes any last vestiges of this consideration.

One of the more noticeable phenomena of the information society is that of convergence of technologies. A website may contain attributes of all three models. In a recent decision of the Court of Session, albeit issued only in the course of an action seeking an interim interdict, it has been held that in terms of copyright legislation, a website should be classed as a cable programme service. The massive

[54] Supra Note 12, p17

investment currently being undertaken to create cable networks in the UK means that television programmes are carried over the same wires as telephone calls. Trails have been conducted to establish the feasibility of introducing systems of 'video on demand', where the contents of a film or other programme will be transmitted to a viewer using the telephone system. Even television transmissions may soon become more interactive, so that, for example, a viewer will be able to place an order for goods or services advertised on television by pressing a few buttons on a television remote control device. As technologies converge, so pressures have emerged for the law to take a similar approach. Both the European Commission and the Department of Trade and Industry have published Green Papers on the topic. The latter document states that:

"Digital technology is rapidly being adopted for the reproduction, storage and transmission of information in all media. This means that any form of content (still or moving pictures, sound, text, data) can be made available via any transmission medium, eroding the traditional distinctions between telecommunications and broadcasting. Already it is possible to receive television or radio over the internet, while digital televisions will have some of the capabilities we currently find only in computers.

The greatly increased capacity and versatility of networks provides opportunities to improve the delivery of existing services and to create new ones. Consumers will have easier access to a wider range of content through various transmission media. They will be able to select the services they want at a time convenient to them and to benefit from enhanced two-way communication through interactivity. The potential benefits to the citizen/consumer, to business and to government are significant.

Our system of regulation faces new challenges as delivery systems adopt a common technology and assume common capabilities. Some new services fall within the remit of more than one regulator, creating a risk of excessive and/or inconsistent regulation. Where an identical service is transmitted over different delivery systems, it may be subject to different regulatory regimes. The development of new services,

and their wide availability, must not be jeopardized by such regulatory overlaps and anomalies"[55].

The key initial document in European which moves towards the information society is the report of Commissioner Bangemann's 'group of prominent persons' to the meeting of the European Council in Corfu in June 1994. Entitled Europe and the Global Information society, the Bangemann Report added a political dimension to previously technically-driven moves towards convergence. Three topics are identified in the report as requiring legislative actions are[56]: 1) intellectual property rights; 2) privacy; and 3) security of information (encryption and information security

Therefore this international trend clearly indicates the need for regulatory framework in the area of free speech, intellectual property especially copyright, privacy and security which are core human rights.

1.5.1 Key Regulatory issues for Sovereign States

Sovereignty is a component that constitutes 'State' under international law along with the other components such as 'people' and territory'. Sovereignty is supreme authority, which on the international plane means not legal authority over all other states but rather legal authority which is not in law dependent on any other authority. Sovereignty in the strict and narrowest sense of the term implies, therefore, independence all round, within and without the borders of the country.

The word "sovereign" means that the state has power to legislate on any subject in conformity with constitutional limitations[57].

Cyberspace is basically a telecommunication network. It is borderless and has caused the 'death of distance'[58]. In relation to the telecommunications sovereignty of a state is governed by the International Telecommunication Convention, 1984.

[55] Supra Note 12, p18
[56] Supra Note 12, p19
[57] Synthetics & Chemicals Ltd V State of UP (1990) 1 SCC 109
[58] Cairncross, Francis, The Death of Distance: How Communication Revolution will Change our Lives, Harvard Business School Publication, 1997

The object of the convention is to facilitate relations and cooperation between the peoples by means of efficient telecommunication services. The term telecommunication has been defined in Annexure II of the convention as follows;

Telecommunication: Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. The definition clearly encompasses the cyberspace as it is now.

With the development of information technology, telecommunications have become much more complex and much more important. The Washington Convention, 1973 and the General Radio Communications attached to the International Telecommunication Convention concluded in Madrid on 9th December 1932 and the European Broadcasting conventions of 19th June 1933 and 15th September 1948 has marked the beginning of attempts to regulate a domain of human activity which by its very nature transcends the borders of territorial state.

India, as a sovereign state has every right to regulate cyberspace but technology makes it impossible for its regulation. For that matter, no country can regulate the cyberspace effectively on its own. One school of thought suggests that cyberspace must be allowed for self-regulation. That is, entities of cyberspace must regulate themselves. It is pertinent to note here the remarks made by John Perry Barlow-

"*Governments of the Industrial world , you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind On behalf of the fiaure, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*[59]*."*

Another school suggests controlling the architecture of Internet for the purpose of regulation. That is Hardware Control and Software control for regulation the cyberspace by the government[60]. This essentially means regulating the manufacturers of computer hardware and developers of software. Regulation of hardware manufacturers might affect their right to trade or business and regulation

[59] John Perry Barlow, A Declaration of the Independence of Cyberspace http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow0296.declaration , visited 13 Feb 2002

[60] Lessig , Lawrence, 'Code and Other Laws of Internet', Basic Books, New York, 1999

of software developers might mean regulation of their right to expression as software is protected under copyright law.

1.5.2 Regulation via Hardware

Johnson and Post assert that because "individual electrons can easily, and without any realistic prospect of detection, 'enter' any sovereign's territory," controlling the flow of electronic information across borders is impossible[61]. It is not clear, however, how this conclusion follows from the premise. First of all, at least for the Internet, electrons are not the relevant unit but Internet Protocol ("IP') packets are. And in order for IP packets to enter a particular territory, certain physical components must be present there. By exercising control over the physical components required for Internet access, the state can regulate cyberspace. At the most basic level, a state can simply choose not to have any connection to the Internet. Of course this means that the state must forego the considerable benefits of Internet communications, including electronic commerce and the increased prosperity it may bring. Nevertheless, states that fear for their ability to regulate the Internet could choose this option. As of July 1996, at least thirty-three states were completely unconnected. At another level, the state can compel the creation of a hierarchical network and then impose control over the top level router in that hierarchy (the gateway host). By controlling the gateway to a subnet, the state can regulate the Internet in its territory. It does not seem relevant whether government control of the gateway components is direct (the government owns the components) or indirect (the government regulates Internet service providers). The point is that where widespread usage of the Internet depends on physical components, a government that controls these components can regulate cyberspace[62].

---

[61] See David R, .Jhonson & David Post, Law and Borders :Rise of Law in Cyberspace, 48 STA. L. REv. 1367 (1996). David Johnson is former chairman of the EFF, and David Post is a Policy Fellow of the ElF. Both are coauthors of the Cyberspace Law Institute. See Cyberspace Law Institute , available at http://www.cli.org, visited 12 Jan 2003

[62] Wu S Timothy, Cyberspace Sovereignty – The Internet and the International system, Harvard Journal of Law & Technology, Volume 10, Number 3 Summer 1997

Of course the barriers imposed by gateway servers may be overcome. First, the user can use normal telephone lines to dial up a provider outside the subnet in question. Second, the user can send or receive encrypted information. Because it is nearly impossible for the government to determine the content of encrypted messages, regulation of such content will be difficult. However, these "exit options" from state control are probably of such a high cost, financially or in terms of necessary, expertise, as to render them marginal to the discussion. The best example of a country pursuing subnet-based regulation of the Internet is China[63]. With the help of several United States companies, China has already built two major government operated intranets connected to the rest of the Internet through a limited number of regulated servers, The China Wide Web, a subnet that will connect all of China's major population centers and provide Chinese language content, is supposed to begin operation soon. It too will have controlled contacts with the internet[64].

1.5.3 Regulation via Software

Another form of content regulation discussed by Johnson and Post is the software barrier, which they predict "will likely to fail as well". But again, the evidence for this view seems slender. There are two loci where software regulation is most effective one at the router[65] level and the other at the end user level. At the router level, Internet regulation is typically accomplished through use of a firewall, or comprehensive system of network filtration and control, implemented typically at a gateway router. A major component of a firewall system is what is called a packet filtration router. Such a router can filter out packets coming from or going to

[63] Freedom of Expression and the Internet in china: A Human Rights Watch Backgrounder, available at http://www.hrw.org , visited on 14 Apr 2005
[64] ibid
[65] In packet-switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point-of-presence on the Internet. A router is often included as part of a network switch. This definition is from SearchNetworking.Definitions, available at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html , visited on 3 Nov 2005

specific IP addresses. This allows the owner of the firewall system to prevent inside users from accessing outside sites, or vice versa. Much of what is considered the "free" Internet at present is already privately regulated through the use of firewalls, typically by corporations. There does not seem to be any intrinsic reason why nation states will "fail" using similar technology. As a part of the subnet system discussed above, China is presently investing considerable energy in the development of a "digital Great Wall of China " for its intranets using firewall technology developed by or with the assistance of United States companies. Singapore also relies on firewall technology, especially proxy servers. At the end-user level, the state can rely on what is called "end-user filtering software" to filter out content. Recently there has been enormous development in the sophistication of end-user filtration systems. Most significantly, wide adoption of the PICS[66] protocol would disallow both sensitive and harmful content thorough content filtration, at least for the World Wide Web. Where every site is reliably PICS rated, private individuals using PICS compatible browsers can elect to receive undesirable content based on several content variables, such as violence, sex, and so forth. Theoretically, such screening can be done with complete accuracy. End user filtering software may also be used to facilitate state control over Internet content. For example, a state could require by law that all browsers made available in the country come equipped with filtration software. This regulation would be easier to avoid than router regulation, because the filtration program would be in the hands of end users. Furthermore, pirated browsers would likely to proliferate. Yet insofar as the bundled filtration software served to increase the costs of exit from the state's rule set, such regulation will be another means by which the state can effectively regulate cyberspace.

China and Singapore furnish the paradigm for effective cyberspace regulation. The point here is not that the regulation exercised by China and Singapore is perfect, of course it is not. What matters is that, by all accounts, these nations have been able to limit the activity of ordinary users. So far these users have accepted the restrictions, or at least have not considered them worth complaining about. It might be argued

[66] Abbreviation for Platform for Internet Content Selection

that China and Singapore are bizarre examples of Internet regulation, made uniquely possible only by a combination of limited Internet connections and a strong government. Or perhaps because so many Asian countries are planning to or already regulate the internet, this can be considered a regional quirk. Yet many of the descriptive claims for cyberspace sovereignty seem plausible only in the face of a highly decentralized network and a limited government. Such features are characteristic of Western liberal democracy in general, and American society in particular; in the world's nations they are absent. There is a reason, then, to question the arguments for cyberspace sovereignty inasmuch as they seem to make sense only in particular contexts[67].

1.5.4 Application of Common Law Principles for Internet Regulation

Common law principles can be effectively used to regulate certain conduct of netizens over the cyberspace. Common law doctrines like Nuisance[68], Trespass[69], Negligence and Strict liability can be applied to control cyberspace activities.

Application of property law, with its ancient roots, to something as recently evolved as the Internet raises questions about the use of such antiquated laws in cyberspace. In spite of its "virtual" nature, the Internet readily lends itself to parallels with real property. Like real property, Internet sites are "fixed" in a cyberspace location. They are identified by an address, have definable borders and are capable of being exclusively controlled. Courts have also recognized these similarities by applying property law to cyberspace in upholding a registrant's property right in an Internet

---

[67] Wu S ,Timothy, Cyberspace Sovereignty – The Internet and the International system, Harvard Journal of Law & Technology, Volume 10, Number 3 Summer 1997

[68] For example Nuisance doctrine can be used to restrict 'SPAM'

[69] California Supreme Court applied Trespass doctrine in Intel Corp V Hamidi (1 Cal.Rptr. 3d 32(2003), available at http://cyber.law.harvard.edu/openlaw/intelvhamidi/ , visited 3 Feb 2004; this judgment was widely criticized citing the reason that in cyberspace every transaction amounts to 'trespass' in the traditional sense;

domain name, enabling claims of conversion for web sites, and enabling owners of web sites to bring claims of trespass to prevent unauthorized access to their site[70].

Critics of the chattels theory fear that allowing web site owners to exert control over who can access a web site and the means by which they can access that web site will have "disastrous implications for basic types of behavior fundamental to the Internet." Since open access to information on the Web has been, and continues to be, the lifeblood of the Internet, some fear the application of antiquated notions of property and trespass may threaten the critical interests of cyberspace. One of the most cited fears is that trespass doctrine, if applied to cyberspace, threatens the legality of the search engines that make finding useful information in the vast repository of the Internet feasible. What this argument fails to take into account, however, is that Internet standards and technology have already ranted web site owners the type of power needed to control access to their web sites. The law of trespass simply affirms and gives a legal framework to these rights[71].

It is also possible to use law of nuisance to prevent unsolicited e-mails, which are popularly known as SPAM, which are flooding e-mail accounts of netizens thereby irritating and harassing them. Sometimes they are also causing the netizens to delete their legitimate e-mails. Law as of now provides for opt-out option only, principle of nuisance can be effectively used to keep the spammers at bay.

1.5.5 Private Regulation

Private entities like Yahoo!, AOL, Google etc will play an increasingly large role in regulating space by prescribing policies for netizens[72]. They can reject or admit members based on their own polices. They also perform censoring speech of their members. They are actually deciding what is good or bad for their members. The

[70] Fricth M David, Click Here For Lawsuit- Trespass To Chattels in Cyberspace, Journal of Technology Law and Policy, Vol.9, Issue1, June 2004, available at http://grove.ulf,edu/~techlaw/vol9/issue1/fritch.html at p 2, Visited on 10 Dec 2005
[71] ibid at p 5
[72] Nunziato C, Dawn, The Death of Public Forum in Cyberspace, George Washington University Law School, available at www.papers.ssrn.org , visited on 2 Jan 2005

point to be noted here is that they are not subjected to any of the checks and balances that we usually associate with democratic governance[73]. And the relationship between these private actors and netizens is of contractual in nature and human rights of netizens cannot enforced easily.

There is no remedy available to aggrieved netizen as violations of human rights can be enforced only against state action. As a matter of legal doctrine, the question of how to apply constitutional or legal norms to private entities implicates the so called state-action or act of state doctrine. The most important question needs to be answered is that whether public-private distinction can be maintained in cyberspace?[74]

1.6 Human Rights in Cyberspace

The Internet is a unique communications medium. Like no other medium before, it allows individuals to express their ideas and opinions directly to a world audience and easily to each other, while allowing access to many more ideas, opinions and information than previous media have allowed. Consequently, there is a vital connection between the Internet and human rights[75].

Through the Internet, citizens from the most repressive regimes are able to find information about matters concerning their own governments and their human rights records that no newspaper may dare print, while denouncing the conditions under which they live, for the world to hear. The Internet allows an intimate look at other countries, other people and other cultures that few before were ever able to attain.

---

[73] Radin Jane, Margaret and Wagner Polk, R, The Myth of Private Ordering: Rediscovering Legal Realism in cyberspace, Chicago-Kent Law Review, Vol.1, 1999

[74] Bellia L, Patricia, Berman Schieff Paul, and Post G David, Cyberlaw: Problems of Policy & Jurisprudence in the Information Age, Thomson/west, USA, 2003

[75] Center for Democracy & Technology, The internet and the Human Rights: An Overview, available at http://www.cdt.org/international/000105humanrights.shtml , visited on 29 Jun 2004

This power to give and receive information, so central to any conception of democracy, can be truly achieved on the Internet, as nowhere before[76].

Further, through the use of encryption technology, citizens can have instantaneous communications with individuals all over the world that are much more resistant to government and private surveillance[77].

On the Internet, citizens are not mere consumers of content but also creators of content. This fundamental shift in power has created a possibility for every individual to be a publisher. Consequently, the content on the Internet is as diverse as human thought. Individuals and communities have been using the new-found freedom online to link, interact and work collectively in this global work space[78].

The effect of access to and use of this global interactive medium has been to promote and defend civil and political rights worldwide. This unprecedented power, however, can be very threatening to repressive regimes. The experiences of communities in different countries so far indicates that few things could be more threatening to authoritarian regimes than access and use of a medium that knows no boundaries and is very hard to control. While traditional methods of censorship - embargoing newspapers and closing down presses - do not work on the Internet, the online censoring techniques that these regimes attempt can be just as destructive[79].

While the Internet is technologically resistant to government control, it is not immune from such control. Indeed, some countries have been quite sophisticated in exploiting the control and surveillance potential to great effect, at least in the short run. Just because the younger generation may know how to "hack" through proxy servers to avoid censorship does not mean that the youth are safe. These actions

---

[76] Balkin M, Jack, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information society, 79 N.Y.U.L Rev1 (2004)
[77] Park, John E, Protecting the core values of the First amendment in an Age of New Technologies: Scientific Expression Vs. National security, Virginia Journal of Law and Technology, Va.J.L & Tech.3 (Fall 1997), available at http://vjolt.student.virginia.edu , visited on 3 Apr 2005
[78] ibid
[79] Human Rights in the Information Society, available at http://rights.jinbo.net/english/into.html , visited on 6 Nov 2005.

should be understood in the technological context - that such hacking is probably obvious to government system administrators, and may make people vulnerable to being identified and prosecuted. Meanwhile, nations around the world are seeking to exploit the surveillance potential of this new medium, including by asserting control over the design and development of communications networks to maximize their surveillance capabilities.

Some of the human rights concerns in cyberspace are related to Civil and Political Rights such as Free Speech, Defamation, Privacy and Economic Rights like right to enjoy the benefits of scientific, literary, artistic work etc discovery and creation are examined in this research work.

(a) Freedom of Expression

The Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), the European Convention and other international human rights agreements enshrine the rights to freedom of expression and access to information. These core documents explicitly protect freedom of expression "regardless of frontiers," a phrase especially pertinent to the global Internet:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media, and **regardless of frontiers**." As stated in Article 19, Universal Declaration of Human Rights.

"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." As provided under Article 19, International Covenant on Civil and Political Rights.

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of borders." As provided under Article 10, European Convention for the Protection of Human Rights and Fundamental Freedoms.

No matter what the means, government restrictions on speech or access to speech of others violate basic freedom of expression protections. In addition to direct government censorship of Internet communications, or privatized censorship, freedom of speech in the Internet is threatened by diverse factors.

Blocking, filtering, and labeling techniques can restrict freedom of expression and limit access to information. Government-mandated use of blocking, filtering, and label systems violates basic international human rights protections. Global rating or labeling systems squelch (crush down) the free flow of information. Efforts to force all Internet speech to be labeled or rated according to a single classification system distort the fundamental cultural diversity of the Internet and will lead to domination of one set of political or moral viewpoints. Diversity and user choice are essential: To the extent that individuals choose to employ filtering tools, it is vital that they have access to a wide variety of such tools[80].

"Self-regulatory" controls over Internet content, which have been promoted by some as an alternative to government regulation, ought not to place private ISPs in the role of police officers for the Internet. With regards to content, what is being suggested in the name of "self-regulation" is not that ISPs should as a group regulates their own behavior, but rather that they should regulate the speech of their customers. This is not true "self-regulation." The role of an Internet Service Provider is crucial for access to the Internet and because of the crucial role that they play. ISPs have been targeted by law enforcement agencies in many countries to act as content censors. While ISPs ought to provide law enforcement reasonable

[80] A Starting Point: Legal implications of Internet Filtering, A Publication of the OpenNet Initiative, available at ,http://www.opennetinitiative.org , visited 12 Feb 2005.

assistance in investigating criminal activity, confusing the role of private companies and police authorities risks substantial violation of individual civil liberties[81].

(b) Privacy

The UDHR, ICCPR, the European Convention and international human rights instruments enshrine the right to privacy. These core documents explicitly protect the privacy of correspondence and communication:

"No one shall be subjected to arbitrary interference with his privacy, family, home or **correspondence,** nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[82]

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[83]

"Everyone has the right to respect for his private and family life, his home and his correspondence."[84]

Privacy is becoming increasingly important for citizens in the information society. Electronic communications can be very easily intercepted by anyone who wants to. Sending an e-mail message is thus the equivalent of sending a postcard. In the human rights arena especially, many matters discussed among NGOs are extremely confidential. Names of witnesses to human rights violations, for example, need to be kept from those who would harm them. Repressive governments commonly use

[81] Sunstein R, Cass, The First Amendment in Cyberspace, The Yale Law Journal, Vol.104, N0.7, May 1995, available at http://www.jstor.org/ , visited on 9 Jun 2006
[82] Article 12, Universal Declaration of Human Rights

[83] Article 17, International Covenant on Civil and Political Rights

[84] Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms

their intelligence services to tap the phone communications of human rights groups and intercept their mail. It is very likely that they are also intercepting electronic mail[85].

(c) Anonymity, Harassment and defamation

Central to free expression and the protection of privacy is the right to express political beliefs without fear of retribution and to control the disclosure of personal identity. Protecting the right of anonymity is therefore an essential goal for the protection of personal freedoms in the online world.

The right of anonymity is recognized in law and accepted by custom. It has been an integral part of the growth and development of the Internet. Some governments are working to extend techniques for anonymity[86]. But at the same time anonymity protection should not be abused. Defamatory speech, threatening speech, hate speech or speech aimed at harassing cannot be tolerated and these can be grounds for imposing restriction on free speech.

But other efforts are underway to establish mandatory identification requirements and to limit the use of techniques that protect anonymity. For example, the G-8 recently considered a proposal to require caller identification for Internet users. Some local governments have also tried to adopt legislation that would prohibit access to the Internet without the disclosure of personal identity.

Governments should not require the identification of Internet users or restrict the ability to express political beliefs on the Internet anonymously. Efforts to develop new techniques to protect anonymity and identity should be encouraged. ISPs should not establish unnecessary identification requirements for customers and

[85] Human Rights in the Information society, Right to Privacy Vs. Government's Surveillance available at http://rights.jinbo.net/english/privacy.html, visited on 11 June 2005
[86] Spencer H, Michael, Anonymous Internet Communication and the First Amendment: A Crack in the Dam of National Sovereignty, Virginia Journal of Law and Technology, 3 Va.J.L & tech (Spring 1998), available at http://vjolt.student.virginia.edu , visited on 3 Mar 2005

should, wherever practicable, preserve the right of users to access the Internet anonymously.

(d) Economic Rights – Democratic rights alone will not be sufficient to realize the full potential of human beings. Economic rights like to right to work which involves physical labor and right to enjoy the benefits of scientific discovery and creativity which are derived from mental labor must also be suitably protected to protect and promote the human rights of individuals. In this regard UN Convention on the Economic, Social and Cultural Rights, 1966 plays a vital role in the development of economic rights of individuals. This convention imposes a responsibility on the signatories under Art.11 to make available the scientific knowledge and its application to all the members of the society. Hence States in order to fulfill their obligations under Art.11 have to recognize and protect the rights of creators and inventors as provided under Art.15 of the Convention which reads as follows;

Article 15 -

1. The States Parties to the present Covenant recognize the right of everyone:
(a) To take part in cultural life;

(b) To enjoy the benefits of scientific progress and its applications;

(c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture.

3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.

4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields.

Commercialization of internet has affected the rights of copyright holders and also created problems for trademark owners. Business method patents have become a reality owing to the nature of the e-commerce business models.

Economic rights in the intellectual field provide for incentive to invent, incentive to disclose, incentive to commercialize and incentive to design around[87].

Human rights discourse in the IPR regime has added a new approach to that analysis of the content and scope of IPR's[88]. As an embodiment of expressional act, IPR has important human rights dimension. Internet assists in the promotion of learning and research and at the same time it might impact upon the rights of copyright holders. Copyright law's basic inclination to support liberty and is an expressional freedom rather than a tool of censorship. Internationalization of intellectual property law with the same purpose, rather than treating it as sheer object of trade is contemplated in human rights philosophy[89].

(e) Jurisdiction – It is not enough for the State to recognize the basic human rights but it should also provide appropriate mechanism for enforcing them through competent courts. To determine the jurisdiction of the courts is very difficult owing to the multi-jurisdictionality nature of the Internet[90]. Determination of jurisdiction for the enforcement of rights cyberspace entities is vital but needs different treatment in this new environment.

---

[87] Chisum S Donald, Nard Allen Craig, Schwatrz F Herbert,Newman Pauline, Kieff Scott F, Cases and Materials : Principles of Patent law, Foundation Press, New York, 1998

[88] Bhat P, Ishwara, Historical Evolution and Development of IPR,1 KLJ [2005] at p, 6 (Kare Law Journal, Issue 1, November, 2005)

[89] ibid at p 7

[90] See generally Yahoo! Inc V LA LIGUE CONTRE LE RACISME ET L'ANTISEMITISME, A French Association, No.01-17424, D.CNo.cV-00-21275-JF, decided by northern District Court of California;

1.7 Protecting Human Dignity in the Digital Age

New technology offers opportunities both to expand and to limit the freedom to communicate and the opportunity to protect private life. For example, new digital networks can provide a high level of security and privacy through the incorporation of such techniques as encryption. The Secure Socket Layer in Internet browser software enables the secure transfer of credit card numbers and reduces the risk that "sniffer" programs will capture credit card numbers. But encryption is not widely used for personal email. As a result it is relatively easy to capture private messages sent over the Internet[91].

New technology can also enable anonymous transactions over the Internet so that individuals can obtain access to information and purchase products without disclosing actual identity. Some object to online anonymity and say that it could be a cloak for criminal conduct. But the question could fairly be asked why individuals should be required to disclose identity when such requirements did not exist in traditional information environments, such as the print world of newspapers and books or the broadcast world or radio and television[92].

Similar questions arise with the protocols for electronic mail services. Strong encryption products could ensure that individuals could exchange private messages with little concern that third parties would gain access to private messages. But slight modifications in these protocols, though such methods as “key escrow” or “key recovery” could enable the routine interception of personal communications[93].

Filtering techniques incorporated in the architecture of the Internet also raise far reaching questions about the character and impact of the new communication services. These programs allow government and private enterprises to restrict access

[91] Rotenberg,, Marc, Protecting Human Dignity in Digital Age, Electronic Privacy Information Center, www.epic.org , available at www.webworld.unesco.org/infoethics2000/documents/study_rotenberg.rtf , visited on 3 Oct 2005
[92] ibid
[93] ibid

to information that is otherwise available. Such methods could limit access to a wide range of important cultural, medical, and scientific information. Already these techniques have been used to limit access to public information[94].

Just as these new technologies are emerging that could significantly influence the future of human dignity in the digital age, technical organizations are playing an increasingly significant role in the policy world. Simultaneously, international organizations are playing an increasingly important role in shaping the policies for the Internet[95].

The quality of human person in cyberspace or in real space involves right to dignified life, personal liberty, Freedom of speech and expression, Freedom of Assembly and association, Freedom of business, trade and occupation, Freedom of religion, Cultural and educational rights and property rights[96]. Protecting and promoting these fundamental human rights in cyberspace is vital for the development of internet and related technologies.

1.7.1 Main Challenges

New technology has always presented opportunities and risks. Industrialization promoted productivity and increased the standard of living in many parts of the world. Industrialization also caused enormous damage to the physical environment. Information technology also presents opportunity and risk. But the main challenges to human dignity in the digital age are not in the nature of the technology itself but in the capacity of individuals acting through democratic institutions to respond effectively to these new challenges.

---

[94] ibid
[95] ibid
[96] Bhat P, Ishwara, Fundamental Rights: A study of Their Interrelationship, Eastern Law House Pvt Ltd, Kolkata, 2004

These new challenges include the commercialization of the Internet, the growth of law enforcement authority, and the globalization of decision making authority. There is also a critical need to understand the appropriate relationship between the two central interests of privacy and free expression.

1.7.2 The Commercialization of the Internet

Since the development of the World Wide Web in 1993, the character of the Internet has changed. The graphical interface has made it easier for many organizations to take advantage of global computer networks, to establish an online presence and to exchange information and ideas in the digital world. Educational institutions, cultural associations, scientific societies and others have all benefited from the dramatic growth of network communications. The web has also made possible the rapid development of new commercial applications that include both business to business services and business to consumer services[97].

Commercialization of the Internet also poses the threat that rights which would otherwise be protected in the political sphere will be turned over to the marketplace and individuals will be forced to pay for services that might otherwise be routinely provided. A critical example is the confidentiality of correspondence. By tradition, communication services have assured the privacy of personal correspondence and personal communication. But commercial forces have found that the records of communications and the transactions generated in the interactive environment are valuable for marketing purposes. Moreover, in the absence of legislation clearly establishing the privacy of new electronic communications, service providers may choose to offers communication services without assurance of confidentiality[98].

Citizens may then be required to purchase confidentiality for routine personal communication or to forgo privacy for commercial benefit. Two classes of Internet

[97] Kasky V, Nike 27 Cal.4th 939 (2002), available on www.findlaw.com , visited on Aug 12, 2005
[98] ibid

users may emerge: the "privacy haves" and the "privacy have-nots." Inherent in the provision of new communications services should be that confidentiality will be protected in law.

Commercialization of the Internet may pose a different challenge to freedom of expression. Here the concern is that market concentration and the consolidation of commercial power could transform the decentralized character of the Internet and reduce the number of voices and the opportunities for non-commercial speakers to participate in the Digital Age. It is therefore appropriate to ensure the balance between these two entities[99].

Next challenge is related to the consumption of digital content in cyberspace. The availability of new techniques to track the use of copyright works in the digital environment; Copyright Management Systems, digital Rights management etc will be used to track the interests of Internet users. Such systems should be developed so as to permit compensation of copyright holders without the compelled disclosure of the identity of Internet users. In this context, anonymity protects both privacy and free expression.

1.8 Hypotheses and Research Questions

For the first decade or so after the development of computer networks and related communications technologies, there was little need for policymakers to pay attention to activities taking place in cyberspace. Back then, the user community was, for the most part, a relatively homogenous group of researchers at universities and commercial laboratories who tended to use the networks to communicate the results of their work or work in progress and not to cause trouble. Once networking and other technologies evolved to the point that ordinary people could easily use the network, and once the National Science Foundation (NSF) lifted the earlier ban on

[99] Johnson E H, Bruce, California's "Creeping Commercial Speech": Kasky Decision Attacks Business Participation in public Debates, available at http://library.findlaw.com/2002/Aug/6/132599.html , visited on 22 July 2005

commercial activities on the networks, policymakers came to realize that they would have to decide how to regulate this new medium of communication[100].

Keeping the above in mind the Hypothesis for the research work is formulated as follows;

" **Legal and Regulatory model for the protection , promotion and enforcement of human rights of cyberspace entities is possible only with the co-operation of sovereign nation-states, who should collaborate, and act together to decide on appropriate best practices, models and legislation to handle human right issues in cyberspace; and to strengthen the international legal system and establish international institutions to meet the challenges posed by new information and communication technologies for the national and international legal regimes"**

Following Research Questions have been raised in order to test the Hypothesis;

(a) **Freedom of Speech and Expression**: - Should the Online world continue to be a freewheeling, unregulated "market place of ideas" or things have gone out of control? If restrictions are appropriate, what steps should be taken? What is the standard of obscenity or indecency?

(b) **Anonymity & Harassment:** - What is the nature of threats posed by online flamers, cyber stalkers and online harassers? What steps might be taken to keep cyberspace safe and to prevent hate and hatreds?

(c) **Privacy**: - Why are electronic privacy rights so much weaker than analogous rights in other venues? Does the public care? Should the public care? How judiciary has responded to the threat of privacy?

[100] Samuelson, Pamela, Five Challenges for Regulating Global Information Society. This paper is based on a presentation given at a conference on Communications Regulation in the Global Information Society held at the University of Warwick in June of 1999.

(d) **Intellectual Property**: - How applicable are traditional copyright laws in an environment where reproduction and distribution of someone else's creations can occur with ease impunity? How right holder interest can be balanced with the rights of the public in digital communication environment? Do information technologies tilting the balance in favour of right holders?

(e) **Jurisdiction**: - With cyberspace existing beyond state lines and beyond international borders, what laws are applicable and in what context? And even if these questions are resolved, how can such laws are enforced? How human rights of cyberspace entities can be enforced?

1.9 Methodology

Doctrinal method has been employed to do the research work. Research involves analysis of case law, arranging, ordering and systematizing legal propositions and study of adjudicatory decisions of legal institutions.

Authoritative books on cyber law, national legislations, statutes of states, Government reports and international treaties were part of the primary source of research and internet, journals, articles, periodicals, Private Institutions reports were used as secondary sources of research.

A critical and analytical method was employed in the analysis of the RIGHTS of the entities involved keeping in view of the judicial decisions of US, European countries and Indian courts.

Internet was invented by the US Government initiative and US courts had the first opportunity to examine and determine the legal issues raised by internet technology. Hence most of the research work uses US court decisions and legislations for the purpose of analysis.

1.10 Significance of Research

The importance of the study lies in the fact that the existing regulatory norms are found to be inadequate to deal with new facts situations created by digital environment. This is clear from the Yahoo! France where freedom of speech and expression issues were involved and while dealing with this issue American and French courts have taken a diagonally opposite view. In addition to free speech issues, privacy, security and intellectual property rights have also become issues of concern for the legal systems. Human rights of the Netizens have to be placed at the higher level of legal norms so that these guaranteed rights in the real world remain intact , when they go 'online' in cyberspace. Legal restrictions that should be imposed on online defamers, harassers etc are also inadequate and there is an urgent need to deal with cyber crimes. The purpose of the study is to address theses kinds of problems to find out possible effective solutions and restricted to the examination of basic human rights.

The Information Technology Act 2000 of India has laid emphasis on e-commerce and has not addressed various other issues such as free speech, right to reputation, privacy, intellectual property rights, jurisdiction etc.

Conflicting judicial decisions of American courts and European courts over cyberspace activities have added to the difficulties of regulating cyberspace.

In this regard it is desirable to examine the existing legal frame work and develop regulatory norms from the global and national perspective. The purpose of the study is to identify the difficulties posed by these new technologies to law and to make an attempt to find out the effective legislative measures required to be adopted to regulate the cyberspace activities.

1.11 Structure of the Research work

There are seven chapters including the first introductory chapter. In the introductory **Chapter 1,** titled as **"The world of Cyberspace",** I have identified some important human rights issues which need to be protected and promoted in cyberspace for the effective utilization of internet technology. Basically research involves around Freedom of Expression extending to other collateral rights of right to privacy, right to reputation and copyright.

In this chapter relationship between law and technology has been highlighted. Technology has been an instrument of social change and internet technology is no exception to this rule. I have also discussed the historical events that led to the invention of internet. Some technical aspects of the internet are also covered. The major features of internet, anonymity and multijurisdictionality have been analyzed to understand the nature of internet. The impact of internet on society is illustrated. The debate that whether we should really need have a cyberlaw between Judge Frank Easterbrook and Larence Lessig is analyzed and an attempt has been made to answer the question. I have also discussed the kind of regulation that may be required to regulate the conduct of cyberspace entities and current thinking among the legal scholars regarding regulation and control. A hypothesis is formulated and research questions have been raised in this chapter. This chapter also includes methodology adopted for research and significance of research work.

Chapter 2, titled as **"Freedom Speech in Cyberspace",** discusses the fundamental human right, freedom of speech and expression in cyberspace and the extent of protection and promotion offered so far and the prohibition of obscene speech in the light of Communication Decency Act, 1996 of US. In this chapter I have discussed various justifications for free speech protection and its importance in a democratic society as a basic human right. The chapter also covers and highlights protection and promotion of free speech under international and national laws. Various case laws decided by Indian courts and US courts are discussed to understand the extent to which restrictions can be imposed on exercising freedom of speech and

expression in India. The chapter also covers various channels that are available on the internet for expression. The highlight of the chapter is the right of adults to indecent material that is largely available on the internet. Invalidation of Sec.230 of CDA has upheld the right of the adults to porn like material. US congress attempt to stall the distribution of obscene material has taken beating by the decision of US Supreme Court in Reno V ACLU. I have also discussed the Miller test of US and Hecklin test of India, to analyze what constitutes obscene material. Various attempt made by the US Congress in protecting the interest of children and women against harmful material have also been analyzed.

Chapter 3, titled as **"Cyber Defamation, Anonymity and Hate Speech",** is an extension of chapter 2 and deals with anonymity, defamation and harassment in cyberspace and analyzes the basis on which restrictions are being imposed on free speech. No right is absolute. Free speech cannot used to harm the reputation of others. But there is a difficulty in drawing the line between harmful speech and the right speech. Over the internet one can be defamed by just clicking a button. The standards used to determine whether speech is harmful vary from country to country. Australian courts making an attempt punish the American defendant is an example in this regard. In this chapter I have focused on the application of traditional rules to online world and examined the difficulties in their application. Right to speak anonymously is another human right that has assumed greater significance with the advent of internet. This right is examined keeping in view with the current judicial trends in US.

Chapter 4, titled as **"Privacy in Cyberspace",** focuses on another important fundamental human right, right to privacy. Protection of privacy interest in cyberspace through existing legislations and judicial decisions and its adequacy is being examined here. American consumers have been actively participating in the commodification of personal data. The tussle between US and EU in sharing personal data is analyzed and safe harbor treaty between US and EU is highlighted. Treatment of informational privacy as human right by EU is the core idea discussed

in this chapter. I have also discussed Fair Information Practices and focused on OECD guidelines for collection and dissemination of personal data. These Principles must be made part of the national law also. It is not the collection of the data that matters, it is the use and dissemination of personal data that might harm the interest of the cyberspace entities. Experience has shown that, through various consumer surveys conducted, consumers can be easily lured to disclose their personal data by offering small gifts by the marketing companies. Legislative attempts by US Congress in the form of Privacy Act have been discussed along with limitations of the Privacy Act. A balance needs to be maintained between marketer's right to collect personal data and the right to privacy of the individuals.

Chapter 5, titled as **"Intellectual Property Rights in Cyberspace",** is about protecting economic human rights of creators and innovators in cyberspace. Protection of intellectual property rights, particularly in the area of copyright is the major point of discussion in this chapter. Most blatantly violated human right in cyberspace is copyright. Majority of the cases that come to the courts are related to copyright violations. Copyright violations have indirectly impacted on trade names and domain names. Judicial decisions in leading cases like Napster, where P2P sharing held to be invalid, and MGM V Grokster are used to identify and analyze the difficulties faced by right holders in the new digital environment. Tilting of traditional balance by the Digital Rights Management System is also discussed. The effects of DMCA on consumers and right holders are also analyzed. Advent of commerce in cyberspace has resulted in granting patents to business methods, which are expressly barred in many countries.

Chapter 6, titled as **"Jurisdiction",** is concerned with the enforcement of human rights mentioned above. It deals with the problem of multijurisdictionality and an attempt has been to suggest the possible solutions to resolve the jurisdictional problems in this borderless medium of communication. Yahoo! France case and John Doe cases have raised lot of issues relating to international jurisdiction. The problem of jurisdiction actually provides an opportunity to create international

agencies to take care of these issues. This again brings back the importance of international law in dealing with the human rights of cyberspace entities. If international law is, in some ways, at the vanishing point of law, the problem of jurisdiction created by the internet technology is bringing back the need and showing the necessity of having a body of international law by its global nature. Taking this point into account I have discussed and analyzed various solutions offered by different scholars which might act as guidelines for policy makers. It is pertinent to note here that promotion and protection of human rights in cyberspace would become meaningless if there is no mechanism to enforce them. Hence jurisdiction assumes greater significance in the study of cyberspace.

In the last chapter (**Chapter 7- Conclusion**), findings of the research have been highlighted. An attempt has been made to answer all the research questions raised in the first chapter. Some of the observation and recommendations based upon my study have been provided under the recommendations in this report.