3.0 GOVERNANCE IN CYBER-SPACE

The control of cyber-crime is a part of the general regulation and management of cyber-space as a whole. Hence the nature and scope of Governance in Cyber-space appears to be relevant to the present study.

Literally governance means the capacity & competency to rule with authority, to conduct the policy and affairs, to regulate proceedings of a territory. The sovereign power of the government is the power to govern... "A nation’s power to protect itself and to exclude harmful influences notably also undesirable aliens from the sovereign’s territory".1 The governance of cyber space means and includes keeping the system ready for use and enjoyment, to take steps for better service, to keep the system in good-repair and properly maintained, to frame and introduce appropriate rules, to resolve disputes if any, to protect the system from unlawful use, enjoyment and unauthorized access, to assist law enforcing authorities against offenders and criminals. In short, govern means—’rule with authority”, conduct the policy and affairs, and regulate proceedings’ of the body concerned [Ref: oxford Dictionary.]

The Cyber Space or e-world has been the technical extension of the real world. And as such it has become a valuable resource of academic knowledge and information, scientific and engineering research, an effective communication media, a space for trade commerce and banking transactions, a place of pleasure, enjoyment and necessity. Case US vs. Thomas 74 F.3d 701 6th*1 Cir. 1996---the website on pornography was held illegal though operated from other state—California. And as such the participation and conducting action and interactions responses by the netizens are required to be done following certain civic codes. These norms are being developed slowly based on values, norms and laws of the real world. The violations of the recognized rules based on the accepted principles take place in the e-world and actually laws on such violations injuring various rights involving life and property, dignity and moral values are common in the cyber space, “which brings us today with nearly 50 million people on-line world wide, is a largely lawless environment that provides the temptation as well as the means to scam, annoy, abuse, harass and generally aggravate others with relative impunity.”2

These violations as in real world are classified into civil and criminal violations. A group of such violations or offences have been grouped as cyber crimes depending upon the gravity, intensity, frequency of the offences. And this present work is confined to this area of cyber crime only. The other group of offences, civil in nature requiring redress are not negligible in any sense and these are to some extent related to the present subject matter of study. But Governance presupposes that there exist entities and communities that have a physical or legal existence as subject of law.”3

---

1 KLAUS. W. GREWLICH- GOVERNANCE IN CYBER-SPACE-- 1999- KLUWER LAW INTERNATIONAL -- HAGUE -- P-19

2 M. A. Banks ----- Web-Psychos, Stalkers and Pranksters----Coriolis Group Inc.- Arizona, USA----P-21

3 Sup—1----------------1999-----------------P-53
The Universal Service concept was taken in 1991 by the National Information Infrastructure program of U.S. to ensure information resources to all at affordable prices. This was the public policy or political program to allow the people to exercise the right to information to the widest possible extent. Thus the right to govern the Internet has always been linked with the right of ownership of physical network. And in this period as well i.e. 1970s and 1980s the telecommunication networks fitted with electronic computers were hacked for the purposes of theft, robbery fraud and illegal gains like credit card fraud etc. Case - U S V Kevin Mitnick the accused was convicted repeatedly in 1981, 1982 1988, 1993, 1997 and 1999 for hacking into public and private computer systems and stealing informations of different organizations like Pacific Bell Watching station (1981) North American Air Defense Command Computer (1982) MCI and Digital Equipment (1988) and so on.

In U S V Robert Tappan Morris(Jr.) 1988 “Robert T. Morris was convicted of violating the Computer Fraud and Abuse Act (Title – 18) and sentenced to three years of probation. 400 hours of community service, a fine of $10,050 and the costs of his supervision”. *3B And his appeal was rejected. He was charged with the offense of damaging the network and online computer by creating and propagating self-replicating worm-programmes in the Internet causing dislocation of cyber activities.

3.1 AGE OF GOOD GOVERNANCE

Cyber space originated first in the age of stand alone computers in 1950s and 1960s. The storage of data in electronic form settings of ‘O’s and ‘1’s was widely in use in 1960s. “Over the last fifty years the people of the developed world have begun to cross into a landscape unlike any which humanity has experienced before. It is a region without physical shape or form. It exists, like a standing wave, in the vast web of our electronic communications systems. It consists of electron states, microwaves magnetic fields, light pulses and thought itself” ....William Gibson called this platonic realm ‘Cyber space” a name which has some currency among its’ present inhabitants”. *3C , The electronic computer very soon after its birth in 1940s became a repository or store house of information in the form of electronic data.

The period of 1950s was the period of scientific and engineering applications of electronic computers. The first data processing electronic computer UNIVAC came into operation in 1951 March. And gradually its potential for data preparation storing and processing preservation and recovery was exploited in 1950s.

---

"There were fewer than 1000 mini computers in use worldwide until 1961. In 1966, nearly doubled to 6700 two years later and nearly tripled the next year to 19000. By 1972 there were 65000 mini computers in use and 150000 by 1974. The explosive growth actually took place in the late 1970s and early 1980s when micro computers or PC was made available at affordable prices. And also that the electronic communication in trade and commerce activities became a part of civil life. And hence the recognition of the electronic data kept in binarocode became a question to be decided in early 1960s. The U.N. G.A. Resolution dated 16th December 1996 (85th plenary meeting on report of the 6th Committee A/51/628) observed, "The General Assembly, Recalling its' resolution 2205(XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade. Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information ... Recalling the recommendation on the legal value of computer records adopted by the Commission at its' eighteenth session, in 1985 ... in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission ... so as to ensure legal security in the context of the widest possible use of automated data processing in international trade".

The recognition of electronic communication data and records and better service were the issues which were dealt with in the 1st age of governance. After this the civil matters relating to trade and commerce like electronic contract, performance and breach etc. were the subject matter of e-governance. Questions involving jurisdictions, enforcement and law making power etc. came up for decision by electronic-community. The issue of cyber crime, management and control thereof appeared thereafter in 1980s onwards and very soon became a serious concern for all connected with the cyber governance.

3.1.1. PRIVATE NETWORKS AND COMPUTER SYSTEMS (UPTO - 1983) The questions involving violations of existing legal norms social and moral values like theft of electronic data, illegal access into stand alone computer or networks, privacy of personal data also arose in 1960s demanding legal intervention solution management and control by national governments and national laws. So the cyber space, though in a limited sense, arose in 1950s and

1960s before creation of the Internet or ARPANET, of 1970. And thus the problem of the protection of rights and prevention of offences in the electronic space or cyber space grew slowly from 1950s. "In the 1940s when the first real computers were being developed today's huge global telephone network, the construction of which began in the late 1800s, had already been steadily growing for 60s years. The first electronic hackers broke into the phase system to make long distance calls without having to pay for them. These telephone network hackers became known as phreakers." 5A, The e-governance thus dates back to the 1950s through the e-storage, processing and records (documents) and took a Prominent step through IPTO (ARPA) in the 1970s.

And e-governance also took shape in the legislations on e-data & records. The stand-alone computers and the private networks in the 1950s and 1960s respectively (as also thereafter) were governed and controlled by their respective owners. There were many private and proprietary networks in USA providing services to their own customers. The IBM developed its' own network named Systems Network Architecture (SNA), the Digital Equipment Corporation had DECNET etc. And each of these proprietary networks used their own computer models and softwares. Similarly the time-sharing systems and work stations developed in the 1960s were also under proprietary control of the concerned authorities the only problem was the recognition of electronic data, message and records created by the electronic devices in its own machine codes.

The successful internetworking of many networks through a single back bone communication line added new dimension to the electronic world in 1970. This was achieved by intensive research work conducted by IPTO under ARPA. In addition to stand-alone private computers and proprietary computer systems and computer networks the cyber or binary coded world opened up a publicly accessible space or electronic world, through on - line computers, having huge data reserve and interactive communications.

LEGAL – ISSUES -

So long the legal issue centred around recognition of electronic data, in mid 1960s and Onwards the other legal issue became the recognition of electronic storage as data bases and electronic messages as well. In the meantime the memory or storage capacity of electronic computers began to expand at an increasing rate. In this regard Gordon Moore, president Intel

Corporation, an electronics engineer predicted that the memory capacity would be double every eighteenth month through research & development. This is known as Moore’s Law. The IKRAM in 1968 reached 64 KRAM in 1980 and by 2001 it reached 256 M RAM. The Perkinson’s Law in this regard says that there is no such things as enough memory. This huge data base reserve in on-line computers raised the questions like privacy illegal access, hacking etc. more seriously than ever before. And so outside the ARPA network various other private and propriety networks were developed in the US and other countries as well.

Hence these networks along with respective host computers thereon, though in an isolated manner formed a part of the world of cyber-space at that time. And at present the intranets and extranets built and enjoyed by corporate bodies also constitute a part of cyber space outside the Internet. And quite naturally this electronic world remain under the absolute control, management and governance of the respective owner user and occupiers subject to due protection against intrusion and other offences through the links if any, with Internet.

The issues relating to cyber crimes in the cases such as Kevin Mitnick, (1981 onwards) R.T. Morris (1988) AT & T crash (1990 none was charged), Vladimir Levin (City Bank NY Case-1994) Richard Pryce 16 yr (Data stream Cowboy) and Matthew Bevan. 21yr www.bogus.net (kuji-1994) Julio Ceasar Ardita. 21 yr (Harvard University Case 1996) etc. were dealt with according to territorial sovereign laws and international co-operation and the law of extradition.

3.1.2. ARPANET WITH A CENTRAL CONTROL

In true sense of the term 'cyber space' it was developed through the successful and interactive networking of four computer centers in 1969-70 in the US. The IPTO under ARPA achieved this through some novel technological break-through like packet switching, Interface Message Processor and the appropriate software. “The Internet began in 1969 as ARPANET an offer by the US Department of Defense to enable defense researchers at various sites across the country try to communicate and collaborate.”6. The A R P A Back bone communication line was nodoubt under strict control of A R P A a defense-body under US Government. But it was very soon connected to many other academic and research institutions-about 200 in 1980 and a thousand by 1984.

6* G R. Ferrera -----Cyber Law --Your Rights in cyber space ----2001---Thomson Learning Ohio - - p-3(2)
APPLICATION OF CODE LANGUAGE AND NAME:  

In order to bring about a technical uniformity IPTO (ARPA) developed in early 1970s a standard code language to be used in transmission through the common back bone line. These are transmission control protocol (TCP) and Internet protocol (IP). This was a timely development for better management of the network traffic passing through different networks using different codes and technologies. Many other international researchers were also engaged to find such a solution to establish uniformity in network communication. ARPA introduced TCP/IP in its own net-work on and from 1st January 1983. This is known as the birth-day of the present Internet.

At this stage, the nature of Internet traffic was the e-mail and news group information services only. So the control on Internet traffic was not so much needed as the technical management of the physical cabling was. “During the second half of the 1980s existing computer networks were largely in government, higher education and big-business to fill this market gap, a number of firms such as Compuserve, Prodigy, Genie and America Online sprang-up to provide low cost-network access and a range of consumer oriented information services from computer games to access to stock market prices. By 1991, it was estimated that these services were being used in half a million American homes, while these networks gave access to Internet for e-mail (typically on a pay per message basis), they did not give the ordinary citizen access to the full-range of the Internet or to the glories of gopher space or the world-wide-web.”

Thus the cyber-space at its' early stage was highly restricted area for common use of the people excepting some news services and e-mail facilities till early 1990s. But with the explosive spread of computers in late 1980s and Universal Access program of US government in 1991 the commercial use of the cyber space began in mid 1990s. During this period, the general control in private networks was fully implemented like ARPA-NET. Easy access and open exchange of information were not possible in early Internet and also in corporate private networks. “.... This is in direct contrast to corporate computer network environments, where the assumption is that all access is denied without explicit authorization and where measures are taken to ensure security”. Also “When the T3 backbone of the physical network was maintained primarily by public funds (through the National Science Foundations NSF net project), the NSF formulated an...
Acceptable Use Policy to establish guidelines for traffic using the NSFnet facilities on the network". 9 And the NSF thus prohibited commercial activities like electronic contracting, advertising or other use for commercial purposes in the network. This authoritative central control and governance in general continued till full privatization of the back-bone lines in the USA. The ARPA formally withdrew in 1990 and the NSFnet also withdrew formally in 1995 and this ended the period of central control on the basis of good governance and better service. “During the first half of the 1980s the growth of the ARPANET had been modest- from fewer than 200 hosts in 1980 to about 1000 in 1984… 28000 at the end of 1987 and to 150000 in 1989 as the multiple research networks and scores of LANs within ARPANET connected institutions became attached to the public Internet. But the Internet was still under government oversight and explicitly restricted to non-commercial use” *10.

The cyber space in its’ pre historic age i.e. before commercialization of the Internet in 1995 was under ARPA control but the global telecommunication network provided link among various computer systems and computer networks. These network links was exploited in this period by expert hackers such as happened in the case of New York City Bank theft (1994) by Vladimir Levin and his team, Credit Card fraud (1997) by Carlos Salgado. of California (SMAK) etc. These incidents however indicated the loopholes in security management of cyber space. The ARPA net work the Internet was under central control of ARPA as to the access and use but the issue of crime management was managed by the state applying traditional legal system.

But this period saw the other ways of Internet governance through better technological innovations, policy formulations, and voluntary-not for profit organizations. The IPTO in this way had formulated and advocated for the TCP/IP in the early 1970s. And this as an open standard was ultimately recognized and accepted by all concerned.

3.1.3. PRIVATIZATION OF ARPA-PHYSICAL NETWORKS

This ARPA net soon developed into a greater than the greatest existing network system connecting many local networks throughout the United States and some continental states in Europe during 1980s. And all through this period of growth the ARPA maintained full control over the backbone communication lines as well as the access to the Internet.

9* B.Falk ---Sybex Inc. USA---The Internet Road Map -----p-20
The National Science Foundation installed a parallel backbone in 1986 and controlled the access right in favour of the research community only “The T3 backbone mentioned above is a critical piece of the network in North America and its' maintenance has not been left to chance. Between 1986 and 1995, the National Science Foundation funded this part of the Internet through its NSF net project”.*11

Thus through the US Department of Defense and the National Science Foundation a central territorial authority of the U.S. played the dominant role in the control and management of the Internet till early 1990s. But in the meantime ARPA withdrew from the network in 1990 and the NSF net also lost its' control over the Network access from 1995 onward. “In 1991, the NSF embarked on an advanced network project named MERIT, to be implemented in 1994. On April 30,1995 as Janet Abbate famous Internet historian reports: “MERIT formally terminated the old NSF Net backbone and ended the US governments’ ownership of the Internets' infrastructure”. Now all the private and public networks could be connected into a single Internet, available for all purposes”.*12.

And in this way the existing rules against commercial use of the Internet (“Acceptable Use Policy”) were relaxed. And by this time the software for browsing the Internet resources was for the first time developed by University of Illinois researchers Mark Andreessen and Eric Bina in 1993 January. This browser software named ‘Mosaic was released in November 1993 for commercial use. The browser software together with World Wide Web software (1991) caused widespread demand for public use of the Internet. The process was slow but definite towards the breaking of government control and authority over the network physical lines as well as general management. The Michigan Educational Reaserch and Industrial Triad (MERIT) was active through NSF net to privatize the internet communication lines in mid 1990s. “As this book goes to press the Internet is making the unsteady transition from public sector to private, the physical networks are being taken over by the telecommunication firms”.*13 The central control of ARPA ultimate was liquidated in favour of the private corporate bodies in 2nd half of the 1990s. The aim of the privatization was not to dislocate the central controlling authority but only to transfer the same from the sovereign to the private corporate bodics. But along with the process of commercial management of the Internet, some other meaningful non-profit. organisations and institutions have become active in the general policy making, management and Governance of the ........

11 * Sup – 9 – 1996 – p – 19
12 * Sup – 10 – 2001 ---- p –174
13 * Sup – 4 - 1996 --- p --- 299
Internet life. And this two parallel processes of profit based commercial management and voluntary non-profit management are important features of the Internet governance "Apparently there is not one entity or organization that governs the Internet, not on the conceptual, not on the operational and not on the content level".\textsuperscript{14} The experience shows that the Internet functions as a co-operative venture of all concerned with direct and indirect support of Municipal Governments. The privatization of the physical backbone lines was completed in mid-1990s in the USA through the withdrawal of ARPA in 1990 and NSF in 1995 and also through the installation of private backbone parallel lines like ALTERNET by commercial bodies of their own, all being inter connected like telecommunication network. "When the NSF net was formally discontinued as such in April 1995, the transition to the new privatized network was successful. It appeared that MCI had become the largest carrier of Internet traffic in the United States. The business arrangement World Com–MCI would have added considerable importance to this market position. Thus the regulatory and antitrust authorities, both in the United States and in Europe, requested the disinvestments of the Internet back bone as one of the major conditions prior to definite regulatory and anti-trust clearance of the World Com-MCI alliance. There have also been other new entrants most notably AT & T into the backbone provision market".\textsuperscript{15} Thus market force was active to introduce private networks in Internet communication system.

The Advanced Network System (ANS) a non profit organization was developed by commercial houses like IBM, MCI (big telecommunication company) and Merit (the Michigmn Educational. Research and Industrial Triad, a non-profit regional network for state of Michigan/ Edu/nsf.net/acceptable use policy) this ANS began to provide backbone access for commercial users as well. Some commercial backbone networks as UUNET, PS etc. were developed in the meantime. These networks however had connections with the Internet via NSF net thus back bone management moved from US Government to commercial houses. The move towards privatization of the Internet backbone lines in the USA had two main objects. The first one was the free access and use of the new technical development in the ICT that is, the Internet mainly for commercial purpose. The second object was the establishment of a commercial control on the Internet as in the case of the global telecommunication network. And as such the giant telecommunication companies like MCI, AT & T, Telestra etc. took much interest and active role in the process of decontrol like withdrawal of ARPA and NSF from the Internet. "Because the NSF did not want to subsidize directly commercial Internet access, the administrative structure of the NSFnet was changed"\textsuperscript{16} And a new entity- ANS–was formed by IBM, MCI & MERIT to provide Internet access.

\textsuperscript{14} * Sup -1------ 1999 ------------ P ----54
\textsuperscript{15} * Sup -1------ 1999 ------------ P ----55
\textsuperscript{16} * Sup -1------ 1999 ------------ P ----54
The free access was achieved through the establishment of commercial Network Access Providers or ISPs like Compuserve, prodigy and America on Line (AOL) etc. in 1980s and 1990s. The access was free in the sense that any one can get access without prior permission of any authority like ARPA or NSF as in early days of the Internet. The Internet started out being ‘free’ in the sense that it was subsidized by government around the world... now virtually all the cost of the Internet in the United States is covered by the private sector, though the fees that users pay in Internet service providers or through advertising revenues that are used to support ‘free’ online access. For example, free e-mail is now available through web browsers from sites such as /http://www.hotmail.com/ and many others.*17

Thus the charges paid by the users do not constitute any profit for any body corporate but is used for the cost of maintenance and servicing of the physical cabling and equipments carrying the electronic traffic. “Cabling is not free. And while it is usually clear who pays for and owns a local network it is not always clear who should pay for installing and maintaining the Internets’ long-distance connections between networks. The cost of connecting a local network to the Internet is usually paid by whoever owns the local network. That owner negotiates a connection with a site that is already connected to the Internet. The owner of the new site pays for the dedicated line that connects it to an existing Internet site. Commercial Internet access providers pass their cost back to their subscribers through monthly charges and hourly usage fees”. *18

The cyber space provides much more than a communication medium. “But it is also the repository for all digital or electronically transferred information and as such, it is the venue for most of what is now commerce, industry, and broad scale human interaction”/ *19 And any part of the huge information resources of cyber space can be transferred in moments to any other desired place over the network and hence the traffic on the Internet is really beyond any control monitoring or recording.

“Currently, traffic on the Internet doubles every one hundred days as sixty million people access the Internet at least once a day. Lawrence and Giles (1999) found in December 1997 that the Internet had 320 million Webpages; their subsequent study concluded that in February 1999, 800 million pages were in place”. *20 Thus the technology of transmission and information processing in the Internet appeared as the insurmountable barrier to impose a central control on the Internet traffic. The Internet traffic is huge in volume and chaotic in nature. The transmission of same document of a website may be found to be transmitted at different parts of the globe. A non-stop transmission of huge data can’t be monitored and recorded, though this is technically possible to record such a large of volume of data every moment.

17* National Academy of Sciences, Washington-Digital Dilemma-2000----p---268(2)
18* Sup --- 9 ------ 1996 ----- p ------ 18
The recording and monitoring the time of use on the other hand, like tale-communication control is also meaningless because the Internet communication does not apply, the point to point contact system like telephone. “Because the forwarding decision is made separately for each packet, the individual packets that make up a single data transmission may travel different paths through the network” *21 This very peculiar technical nature actually stood on the way of making any Internet company at global or national or regional level. Thus one object of Internet privatization to impose commercial control in any way could not be achieved. “The Internet has no president, chief operating officer or pope. The constituent networks may have presidents and CEOs, but that’s a different issue; there is no single authority figure for the Internet as a whole” *22 Though however the object of commercial control of the Internet traffic could not be reached, the commercial activities like advertisement, publications, communications, sale purchase transactions, information sharing so many others are widely conducted in this system “Much business is conducted directly over the public networks today. Software is distributed, news is delivered, banking is transacted, book and music sales are finalized. In some communities you can even place pizza-delivery and taxicab orders over the Net. These and other activities are rapidly building cyberspace into a significant market place.*23

The ultimate effect of privatization thus specifically went in favour of the common users named as netizens as a non-profit technical system and to some extent for the for-profit business community also. “During 1994, the number of hosts on the Internet more than doubled form 2.2 million to 5.8 million and in 1995, it almost tripled to 14.4 million. The impact of the commercially available Internet quickly began to transform commerce, industry and the basic ways of life. With its appearance, the infrastructure of the Electronic century was in place so consider 1996 as the cutoff date of this history”. *24

And the governance as of proprietary right like that of a body corporate or sovereign power finds weak ground in this new situation to stand upon. “In many ways the Internet is like a church; it has its council of elders, every member has an opinion about how thou should work and you can either take part or not” *25 The matters related to Internet support system are actually maintained by some voluntary non-profit organizations or autonomous bodies though the other parts like host computers and L A N are owned by private people, the communication lines are offered by Telecommunication companies on lease or cost of service basis on commercialization of the Internet in 1995 the e- Commerce issues, cyber torts , cyber frauds and new ranges of cyber crimes came up with growing intensity and frequency. The transborder e- commerce issues, however found a ready legal basis ......

21* Supra-17----Edn --2000--p-264
22* Ed Krol – The Whole Internet Users Guide & Catalogue
23* Sup – 19 – 1995 ----P ----9
24* Sup – 12 ---- 2001 – P – 174
25* Sup – 22 –1994 ---- P -- 16
through conventions international agreements, principles, rules (like choice of law, Minimum contact) and also through case decisions on trans border transactions and commercial activities.

In the case :- International shoe Co-versus-Washington 326 US 310(1945) the court observed that companies voluntarily doing business and taking advantage of the benefits and protections offered by the state should also be liable in the state. But in another case :- Asahi Metal Industry Company (Japan) 480 US 102(1987), the minimum contact or commercial nexus was not considered to be strong enough to find jurisdiction to try foreign Taiwanese plaintiff’s case in California US. The Japanese Co. (Asahi) was sued by one Taiwanese manufacturer as the Japanese Co. had commercial activity (stream of commerce) in California. It was observed that higher jurisdictional threshold was required to over come higher Jurisdictional barrier. Case: Asahi Metal Industry – Vs – Superior Court (Cal) 1987.

Similarly in the case : Core Vent corporation (California) Vs-Nobel Industries A/B II F.3d 1483 9th Cir, 1993 it was observed by the District Court California that non-citizen defendants could not be tried due to lack of personal jurisdiction. The defendants were publishing false statements causing confusion and damage to the plaintiff’s business of dental equipments. In case of non-commercial areas the wrongs resembling to criminal offenses in cyber space uniform rules could not be reached in the past years of the Internet. In the case :- Playboy Enterprises Inc – Vs – Chuckle berry publishing Inc. 939 F Supp. 1032 (S.D.N.Y. 1996), the website operated from Italy could not be controlled by US laws simply for the reason that it was accessible to all including US residents.
3.2 TOWARDS SELF-GOVERNANCE IN CYBER-SPACE

The privatization of back bone communication lines of the Internet in US was started in 1995 onwards and this opened the commercial use of the Internet. " ............ the Internet has changed dramatically in the last few years. The commercial sector is the fastest growing portion of the Internet user community. The North American Communications companies and the large regional networks have established alternate network routes that bypass the NSF net system." * 26.

After withdrawal of defense control the Internet lost the central authority or governance. This was fully exploited by commercial sector to provide easy access to the Internet for common people. And the number of computers connected to the Internet grew rapidly in millions. The universal access policy was taken up by US Government in 1992 connecting 1 million computers to the Internet. And by 1995, 6.5 million computers of about 62000 local networks were put on the Internet. And this growth rate continued through all along till date.

However the Private control of the existing communication lines, free commercial use of the cyber-space and explosive growth of on-line connections could not establish any central body to govern the fast growing cyber world. And obviously the Internet users and computer professionals themselves came forward to manage the situation on the basis of good wishes, proper maintenance and use of the Internet. “Apparently, there is not one entity not on the conceptual, not on the operational and not on the content level........ There is a recent history the performance of these coordinating functions, pertaining to the Internet that shows some involvement of government agencies, but mainly an array of quasi-governmental, and non Governmental bodies . The U.S Government in many cases, has handed over responsibilities to these entities through contractual or other arrangements.” * 27.

And these Internet bodies, essentially non-profit organizations recruit their members from academic sector i.e. Professionals and technologists as volunteers.

“The basic premise of Internet ethics is that no user should do anything that would place at risk the network, its’ users or the agencies that contribute resources to the Internet.” * 28.

The ARPA authority did not impose TCP/IP on the network users as a matter of right but left it as an OPEN STANDARD for users with the purpose to have a uniform code language for all network transmission. Ultimately it was voluntarily accepted by all networks.

28* Supra – 9 -------- P – 20------ Edn. – 1996.
"What lays behind the success of the Internet TCP/IP is the principle of “Open Standards”. That means the protocol is first written, then freely distributed to anyone who wants to use it. Overtime, the protocol is revised, building upon the experiences of the users and not just the original authors.” * 29. Thus the governance in the sense of sovereign power or corporate body was not applied to the cyber – regime.

The different regional parts of the global Internet physical cabling are maintained by different national governments and sometimes telecommunication companies having the telephone lines also form an active part of the Internet. The communication satellites are orbited, by both the national governments and communication companies as in the case of I N T E L S A T. (International Telecommunication Satellite). “It is not possible to use communication through ground methods beyond certain distance. This is (i) due to fading of signals which can not be amplified without noise and (ii) due to geographical reasons like sea, desert, mountains etc. In such a case communication can be done through satellite. The satellite acts as a reflector...... At present nearly 100 communication satellites are in stable “Parking Orbits” approximately 22,300 miles above the earth. These satellites are operated by private companies such as American Satellite Company, AT & T, COMSAT, Intelsat, RCA, Satellite Business Systems and Western Union. These companies sell communication service to customers”. * 30

These geo-stationery satellites placed above the Equator receives radio signals from one place and then reflects back to some other place to be received for local transmission. These signals carry data, voice and video communication at both national and international level.” Governments and international organizations, business firms, business alliances and commercial interest groups and federations, but also civil society entities and, of course, the individuals/citizens/consumers are the actors in the emerging cyber space”*. * 31 Also that “But neither the national governments nor the international telecommunication companies lending their physical cabling and / or satellite system for the Internet traffic, can establish any controlling official authority over Internet, perhaps for their very nature of regional limitation and profit-motive functioning system. “The Internet is not government controlled, but neither is it controlled by commercial interest. It is global in nature but there are no treaties or international agreements that govern it”. * 32 There is no Internet Inc as a corporate body as such any where in the world to rule the Internet with any authority, what so ever.

31 * Supra – 1 -------- P – 26(3)---- Edn. – 1999.
32 * Suresh T. Viswanathan – Bharat Law House Delhi --- P – 6
However various national governments and different telecommunication companies actively provide assistance and support systems for the Internet. "The constituent parts of the Internet are owned by third parties. Thus, hosts and routers are owned by public and private parties, whereas the transmission facilities are most often owned by the operators, the telecommunication companies"*32A. In 1980s Advanced Network Systems (ANS) a non-profit entity was developed by IBM, MCI and Merit to sell back bone access to the users. But a co-operative effort has emerged among three distinct sectors namely voluntary non-profit NGO like organizations, governmental or quasi governmental bodies and the third commercial houses (corporate bodies) in order of merit of functional activity related to cyber-management generally. They operate in the areas technical supervision to keep the system running and in good repair like Internet Engineering Task Force (IETF) Inter-net Architecture Board (IAB) etc.

They operate also in the area of civil (system) administration like Domain Name System, protocol development dispute management on domain name issues etc. like INTERNIC, IANA, NSI, ICANN, world wide web consortium (www.w3.org) etc. "Sovereignty over this new world is also not well defined. Large institutions already lay claim to large field, but most of the actual natives are solitary and independent, sometimes to the point of socio-pathy". *33

The Cyber-society is growing in a way similar to those prevailing at the dawn or civilization-lacking the concept of sovereign Government. Other than voluntary organizations, some academic works like ASCII (American Standard Code for Information Interchange) code, the symbols used for Internet communications such as smile =), Crying : (, ta – ta for now = T T F N. devil = }>, angel = O :), amazed = O etc. have become popular and used as standard communication code.

And thus voluntary non-profit bodies and their contributions actively maintain Internet system as a co-operative venture which is neither a government nor private sector enterprise in the traditional sense. And a sense of responsibility, self restrain, better service, good wishes and just freedoms are the guiding principles in the Cyber-society which is the new face of the old society. This emerging Cyber-life based on self-regulation remains to stand the test of time in coming days. And it is by this time, clear that an order is slowly coming out of the chaos of information, technologies, rules and regulations, right and duties, right and opportunities, for profit and not for profit activities, and so many other issues raised in Cyber-space. It is observed that ------------------------. "It is not necessary to bring in criminalisation and State force in regulating each and every institution. Alternate strategy of self regulation is equally important. Such a strategy is the strategy of adopting soft-laws for self regulation by the users and service providers of the Internet". *34

32a* Sup -1 ----- Edn ------ 1999 -------P------37
33* Sup --- 3c – 1996 ----- p --- 14
3.2.1 VARIOUS CONCEPTS ON SELF GOVERNANCE IN CYBER SPACE

The cyber space is the creation of highly sophisticated technologies and theories of 19th & 20th C like micro electronics, software technology, electronic computing (Pennsylvania Technique), Boolean theories, Information theory, packet switching technology, communication and transmission devices, wireless and satellite system and some others. "............... The Internet and cyber space may be also approached as a paradigm, a manifestation of a new, global, more holistic world view, an amplification of mans intellectual tools, a collective interactive experience of brainpower". * 35 But the fallacy is that this newly acquired/discovered territory though created by the man is also a place of mystery to himself. Even the best informed person can't give a reliable picture of cyber geography. "Thus we might look to Internet as an emergent paradigm. ‘One whose delineations are neither fully realized nor defined, but that by virtue of its' obvious imaginative power characterizes and reshapes all it touches’. * 36 The cyber space on the other hand is expanding every moment beyond the knowledge of any person or office whatsoever.

Millions of users throughout the globe are adding or changing the contents of existing materials or experimenting something on the Net. And as there is no Central computer or office to record and monitor cyber activities no one can have any idea about the growth of the space. "The consequences of ‘self accelerating technologies’ and of unlimited band width in human interaction are impossible to predict". * 37 The cyber landscape is not very much clear to the technical world itself the creator of cyber space. "The cyber space is also unfamiliar because it permits action at a distance. Computers can be broken into from half a world away, for instance ....... Cyber space is an odd new world, where our ordinary intuitions are not always reliable". * 38

The cyber infrastructure specially the transmission lines, satellite and wireless network are so pervasive and widely distributed through out the globe that no territorial authority or a collection of them can manage the cyber space as whole. "Because the Internet is a coalition of networks throughout the world no one organization owns the Internet". * 39

35* sup 1 ------1999------p53
36* sup 1 ------1999------p29
37* CSIS ---- 2001 ---- P ---- x
38* Sup ------17----2000-----P----49
39* Sup----6----2001-----P----8
"Unlike commercial networks (such as CompuServe or Prodigy), the Internet is not run by a central computer or computers; its resources are to be found among thousands of individual computers. This is both its greatest strength and its greatest weakness. Because of this broad base its virtually impossible for the entire Net to crash at ones even if one computer shuts down, the rest of the network, stays up".

* 40"Governance normally presupposes that there exist entities and communities that have a physical or legal existence as subjects of law". * 41 So far it is understood that Internet can't be kept under any corporate management like telecommunication companies, broadcast or television system nor under any sovereign control so far the international network of the Internet is concerned.

"As a result, the Internet is a virtual network which in principle is not regulated as such; subject to regulation however is the underlying infrastructure over which global information networks operate. In certain cases, parts of the underlying infrastructure, for instance so called back bones, (high capacity lines), are dedicated to Internet traffic". * 42 Managing the simple legal issues has been difficult as no clear and effective Jurisdiction can be asserted by any authority or legal system due to cross border interactions without any control system as in telecommunications system. “The legal concerns that affect us domestically are the same concerns that affect our use of the Internet internationally. Issues regarding privacy, security, jurisdiction, trade marks and commerce are all affected by our expanding use of computers to communicate, collaborate and trade”.* 43

No legislation can be effective as the entire humanity is divided into many territorial sovereign legislatures. “Indeed, all the legislation in the world, in all the Jurisdictions that ever existed, wouldn't be able to reliably control behavior on the Net”. * 43a However various principles and concepts on governance of cyber space are in operation with varying degrees of success, the Rule of Law is a practical necessity to have a uniform treatment of all cases of violations of social values, moral rules property rights, civil liberties and human rights in all forms. The concrete rules and procedures as to the governance of the cyber-space are in the stage of formation only and these could not crystallize due to the strong global character of the Cyber – space. The trans - border communications, surfing, downloading and publishing activities have become so pervasive and irresistible that no individual or a group of municipal governments can frame definite rules due to lack of territorial jurisdiction over it. So the concept of sovereign control over cyber-space does not work at global level. “No one owns the Internet as a whole and it is remarkably free of net-work-wide regulation. Certainly all the parts

40* Sup - 3c ----1996 --p----4
41* Supra -- 1 ------- 1999 ---------- P - 53
42* Supra -- 1------- 1999 ---------- P - 38
43* Supra -- 6------- 2001 ---------- P - 11
43a* Supra -- 3c------- 1996 ---------- P - 115
of the Internet (individual networks, some local and some quite large) are owned by someone and the owners of local networks set policies for the appropriate use of the resources they make available to the larger community". *44 Various ethical rules have been formulated for the user community specially in the areas of Privacy Accuracy, Property, Accessibility (PAPA). "Organizations such as Internet corporation for Assigned Names and Numbers (ICANN), Civil Society Internet Forum and Computer Professionals for Social Responsibility (CPSR) have formulated various recommendations and guidelines that seek to regulate the impact of web technology on Society". *45 The general public interest relates to security, human dignity and privacy. In ACLU Vs Janet Reno S. Ct. 1997 the website running pornography program was fined and declared illegal by another state.

All the actors in Cyber space management like governments, Telecommunication Companies, Inter governmental bodies, Non governmental organizations, academic and research institutions, & business houses, technical community and common users, service providers, media companies are acting co-jointly on the basis of mutual co-operation "Regardless of who foots the bill, the network is a co-operative venture and users of the Internet are in fact members of a world wide community. This community survives with very few rules and most of those are simply based on common sense". This heterogeneous community is actively participating in keeping the cyber space in proper order without any enforceable legal contract in traditional sense. They cooperate from an inherent urge of keeping the system in order.

The other premise of making cyber policies may be simple voluntary agreements among different actors and participants. "We reject kings, presidents, and voting. We believe in Rough Consensus and Running code – Internet Engineering Task Force Credo". *46 The global nature of cyber space comprising diverse socio-political and economic systems can survive only through voluntary agreements and not by use of compulsion and pressure. The principles of justice equity and good conscience also provide a sound basis for formulating cyber policies for the cyber community. In the absence of sovereign control and corporate authority over cyber-space the cyber community will be guided by the principles of justice, equity and good conscience. "The Internet’s open, consensus driven, academic roots clearly influenced the current configuration, creating challenges for commerce and law". *47 – And also it is observed, “Indeed the rise of the Information age has brought about a good deal of 'endism'. New technology is widely predicted to bring about, among other things, ---- the end of politics, the end of government, ..... the end of the nation state .......”. *48 A complete autonomy for cyber space on the basis of self-rule provides another concept emerging in the subject of governance. “The different stakeholders having interests in cyber space i.e. economic actors, such as .........

46* Supra – 6 -------- P – 4--- 1996
47* Sup – 6 – p--- 12 --- 1996
trans national enterprises and international industry confederations or civil-society entities such as various NGOs. Enter into the scene of international law not only as subjects of law to be regulated, but also as self-regulators and as partners in the elaboration of hybrid instruments that may contain principles and rules conceived as “multi track”. Because they are addressed to governments as well as to economic and societal actors. * 49. So the concerned quarters are in search of alternative concepts procedures and rules for cyber governance. But rule of law or rule of social values or rule of moral norms or agreed upon public policy or a suitable combination of all these appears to be necessary as the basis of cyber-governance. “We do want rules, we just don’t want rules imposed by centralized powers that tend to flout their own values, at times in secret. In stead of telling the governments to keep out, we are fostering initiatives that will let individuals perform some of the tasks of Net - Governance. …” * 50.

of late the Internet as a technical system is maintained by different sovereign governments, several non-profit autonomous bodies made of computer professionals and user community, like ISOC, IAB, ILPF, CERT and so many others. A collaborative atmosphere prevails without any written agreement. “Governments and international organizations, business firms business alliances and commercial interest groups and federating but also social entities and, of course, the individuals/citizens consumers are the actors in the emerging cyber space”. * 51. These governmental, intergovernmental and non-governmental entities, academicians, users and others also formulate some rules, conventions norms, values and ethics for the Internet users without exercising any sovereign power or corporate authority. Internet Governance in which direction is till now really an issue of speculation of all concerned. “The two fold challenge is for us to create community standards for this new global net space and make those standards enforceable by rewarding good behavior rather than by punishing bad (or perhaps some combination of both). * 52.

Three major forces namely corporate bodies, sovereign governments and non-profit autonomous bodies are found to be active in cyber governance at present. “Not everybody is convinced that governments have an organizing and ordering role to play in the transition to cyberspace”. * 53 This new and emerging trend of non-profit voluntary activity by common people the user community stands as a potential governing power for the cyber………..

49* Supra – 1- Edn. 1999 ------- P – 319
50* Sup – 3c ------------ 1996-------P – XIII.
52* Sup – 3c ------------ 1996-------P – 16.
53* Sup – 1 - ---- 1999 ------- p ---- 8
space. And in no way their role and importance can be ignored at present and in near future in general management of the cyberspace including management of cyber crime as will be clear from discussions and analysis and observations to follow.

3.2.2 Autonomous bodies operating in the Cyber Space

The proprietary state control over the North American back bone communication lines through the ARPA has been diluted step by step in the 1990s. The formation of Milnet a separate network for the Military use in 1982 freed the ARPA – network from strict Defense (US) Control. And ultimately ARPA formally withdrew in 1990. The National Science Foundation (NSF) took up the management of the back bone communication through NSF net in 1986. The NSF net was then a policy making body to control and manage the Internet affairs. But this body also withdrew in 1995 in favour of full commercial use of the back bone lines. And the Commercial Communication Companies established parallel communication routes for network traffic in the mid – 1990. But through this dilution of state proprietary Control over the Internet and full commercial participation in the internet use and building parallel communication lines, no effective Central governing body could be formed. “It is always important to remember that the Internet has no centre, no headquarters or central administration and that individual transmission may, due to a number of factors be rerouted through multiple different providers”. *54.

The Internet space has covered the entire globe and hence any sovereign territorial authority finds no powerful basis to govern the Cyber Space as a whole. In this complex situation arising out of the absence of any central authority, a number of autonomous non profit NGO – like entities have cropped up to maintain the functioning of the Internet Space some organizations are also functioning as a part of some national government but on the principle of non-profit general welfare program. “Because the Internet is a coalition of networks throughout the world, no one organization owns the Internet. The Internet Society oversees boards and task forces that deal with network policy issues. Among these are the Internet Engineering Steering Group, which is responsible for final approval of Internet standards and the Internet Engineering Task Force, the protocol engineering and development group. The Internet is largely self policing – networks that do not conform to the norms of the Internet are cut-off from the rest”. *54a

---

54* Supra – 1 -------Edn --- 1999 ------ P – 86
54a* Supra – 6 -------Edn---2001---- P – 8
The US government had largely transferred responsibilities to different entities for Internet management, administration, and control. The Internet traffic pass through various networks and various state-jurisdiction. The technical coordination as well as overcoming the political barriers are done jointly by governmental and non-governmental efforts. "There is a recent history of the performance of these co-ordinating functions pertaining to the Internet that shows some involvement of government agencies but mainly an array of quasi governmental and non-governmental bodies". * 55

Other than the sovereign governments and commercial sectors— the civil society groups, NGOs— IGOs and quasi governmental bodies have been active in Cyber Space essentially in Civil management and administration of Internet support systems like Internet Address, names and numbers, Domain Names, etc. "The Internet Society (ISOC) is the most comprehensive of the new Internet organization. ISOC is a non-profit professional society founded in 1992. It organizes information events and working groups and co-ordinates some of the efforts of other Internet administrative bodies". * 56 The Internet address is important for the identification of a particular network and a computer on line. This is managed and administered by a non-profit organization the Internet Corporation for Assigned Names and Numbers (ICANN). This was incorporated in 1999 in California US. ICANN maintains a co-ordinating function as to IP address, domain name system management, space allocation etc.

The National Science Foundation Network founded in mid-1980s was administered by a non-profit network organization of state of Michigan— named MERIT (Michigan Educational Research and Industrial Triad) These autonomous bodies were essentially formed by academicians, research groups and technical persons— having the common intellectual goal of a cyberspace free from political and commercial domination. And as such these groups easily worked in a coordinate manner. "The Internet is not government controlled but neither is it controlled by commercial interest. It is global in nature, but there are no treaties or international agreements that govern it. The only inroad so far seems to be the efforts of WIPO to be recognized as dispute resolution mechanism provide". * 57.

3.2.2.(A) - CIVIL AND TECHNICAL BODIES

Major part of the essential services in the Internet official administration are performed by non-profit organizations as follows—
1. The Internet Society (ISOC) - It is a non-profit organization

55* Sup - 1 ------Edn----2001------ P - 54
56* Sup - 1 -------Edn--2001----- P - 55
57* Sup - 32------Edn----2001----- P - 6
established in 1992. The ISOC has most important role to co-ordinate various other voluntary organizations doing administrative jobs. Thus the (IESG) (Internet Engineering Steering Group) and IAB – (Internet Architecture Board) work under ISOC.

2. **NIC** – or **INTERNIC** – Internet Network Information Center – This body registers the local networks for Internet connection. “The Inter NIC supplies the portion of the address that identifies the local network and gives the local networks administrator a range of addresses that can be assigned to individual hosts within the local network”. * 58 The Internet address a powerful identifier, is a 32 bit number chain having four different number separated by periods like 114.82.101.32 where each separate number ranges from 0 to 256.

3. **Inter Agency Task Force** (IATF) was created in 1997 February by US Government to administer Domain Name System (DNS) of the Internet addressing. This Domain Name actually matches with the numerical IP address to identify a particular network and its’ computer. The DNS was first started in 1984.

4. **ICANN** – Internet Corporation for Assigned Names and Numbers – This body was founded and incorporated in 1999 in California US. It performs the central co-ordinating functions regarding, IP address, domain name dispute management, space-allocation and like others.

5. **Network Solutions Inc** – **NSI** – It provides for registration and administration of Domain Name System for dot com, dot org, dot net. NSI also decides disputes on domain names.

6. **IANA** – Internet Assigned Numbers Authority – This entity manages Internet names and numbers globally and it works in collaboration with the Inter NIC and APNIC (Asia Pacific Network Information Center).

7. **IAB** – Internet Architecture Board – and

8. **IESG** – Internet Engineering Steering Group function under the Internet Society and look after technical issues of the Internet functioning.

Other than the recognized and formal bodies like IANA, ICANN, NSI etc. doing official jobs and functions giving IP address, Domain Names, protocol management etc. many other civil society associations and groups have been formed such as EFF, ILPF. These informal bodies or groups are actively participating in making, new standards, norms and rules for the cyber space through discussion debates and declarations.

---

58* Sup ---9 ------ Edn ------1996 ------ P -----52
9. **Electronic Frontier Foundation** - EFF - It is a civil liberty organization established in 1990. EFF carries on extensive research work on cyber life and it is engaged in formulating - standards, norms and rules for the cyberspace. (http://eff.org)


11. **Electronic Privacy Information Centre (EPIC)** - Washington DC - Info @ epic.org -

EPIC was established in 1994 as a public interest group. EPIC carries on research on human rights, civil rights. Cyber policy and governance of the cyberspace generally.

12. **World Wide Web Consortium** - W3C - The MIT laboratory of Computer Science and the French National Institute for Research in Computer Science (INRIA) jointly founded this research body in 1995 to administer web protocol development and Internet software. This body however works in co-ordination with other / research centers on the subject. http://www.w3.org

13. **Center for Democracy and Technology** - CDT

   Washington - http://www.cdt.org -

   "CDT is a non profit public interest organization. The mission of CDT is to develop pubic policy solutions that advance constitutional civil liberties and democratic values in the new computer and communication media". * 59 CDT Carries on research on different issues regarding public policy, civil rights, privacy in cyber space.


IGP is a consortium of academics working on civil liberties and Human rights in the Cyber Space. In recent past - August 2005 organized strong protest against US intervention in ICANN - Internet autonomy.
In the subject of law and order, safety and security in cyber life several voluntary organizations have also cropped up, like those in the civil administration and management of the cyber-space. These non-profit and non-governmental bodies assist the victims of cyber offences by way of guidance to take preventive measures, to track and trace the hackers, and so others, some government and inter-government organizations are also actively working globally against cyber-crime.

1. International Web Police (Florida) It was established in 1986 as a non-profit organization. It provides round the clock Emergency Assistance as international agency on security in Cyber space. ([www.webpolice.org](http://www.webpolice.org)). *Computer Security Institute – CSI – at [http://www.gocsi.com](http://www.gocsi.com) & [www.scamwatch.com](http://www.scamwatch.com)


3. ISPMP – Information Security Permanent Monitoring Panel of UN: This body was formed by the United Nations in Sep. 2002 to study on the emerging threat of Information & Communication Technology.

4. CERT – Computer Emergency Response Team – It was established by US Defense Department to deal with cyber-crimes.[www.cert.org](http://www.cert.org)

Cyber space as such is a new Domain distinctly different from existing physical world and related concepts or governance. Hence a new approach other than the traditional concept of sovereign-command duty-sanction appears to be necessary to fit this new regime. “The emerging strategic paradigm(soft-power) may also be about exerting leadership not necessarily control over communities or individuals and organizations by actively informing but also respecting and taking advantage of the intelligence of others”.* 60.

The new approach may thus frame broad outlines of policies on the basis of rough consensus on public good, basic human rights and the scope of technical innovations to come.
Having no authoritative government, governing body or body corporate as such for the cyber-space as a unity, different national governments have turned to make laws in their own ways on different cyber issues like e-commerce civil rights & liberties, IP - rights, cyber-torts and cyber-crimes for her own citizens. Cyber law as such is the law governing the use of computers and the Internet. But it is in a process of concretization, because the cyber space itself a very new concept and unfamiliar to present legal community of the world. “Governments around the world, struggling to deal with this new ‘place’ and its many effects, are scrambling to regulate the Internet”. * 61 The scope of legislation is limited as cyber space is a unity, once any one takes access he reaches any and every place on the globe. There is no legislative body in the world as such to make universally applicable legal provisions. The individual sovereign states find it injurious to enforce any law other than its own.

Hence the provisions of a treaty or covenant or guideline of UN are first included in the respective state legislative code and then enforced in the territory concerned. “While well-established legal principles and the standards of physical communities give structure and coherence to uses of conventional media such as newspapers, books, and telephones, the new digital media don’t so easily fit into existing frameworks What Jurisdiction’s laws can hope to apply to a medium that’s both nowhere and everywhere at the same time”. * 62 Different states have different social values and standards which differentiate again the legal structure of one country from the other. And political and economic rivalry among nations create insurmountable barrier for uniform political and legal system. So legislation for cyber space in a sense is difficult and impracticable. “It is also an area where legislation is not always easy to craft. For example, cyberspace currently hides virtually all physical cues about a person, making identity difficult to establish. The lack of cues matters for a variety of reasons, including enforcement. *63 The subject of law is always a human being and in cyberspace the actor though a human being (sometimes a robot computer) gives no identity to the other side reacting with him. The invisibility and intangibility actually stands on the way of application of the law in Cyberspace.

However the law enforcing agencies in different countries are active to control the user-community of these respective states and as such have to wait at the border expecting response and co-operation from other national administration. This is a growing difficulty in the area of cyber-investigation and detection. The question of jurisdiction and forum and enforcement etc. stand as a series of question marks before the law.........

61* Sup -----3c ------- 1996-------P-----170
62* Sup -----3c ------- 1996-------P-----7
63* Sup -----17 ------- 2000-------P-----49
“In cyberspace, there are not only no national or local boundaries to contain the scene of a crime and determine the method of its prosecution, there are no clear cultural agreements on what a crime might be”. * 64 However the other side of the game is the demand of safety & security of cyber-space. So the law of each state is active to make – legal provision to respond, investigate, identify and prosecute offenders – as far as practicable. “Global information networks however, are inherently indifferent to geographic – political boundaries. How is it possible to achieve national public interest objectives under conditions of trans border network and possibly market convergence? * 65 And obviously the success of the national legislation will be achieved only to a limited extent.

Due to the peculiar nature of the cyber space, the scope of effective legislation (complete code) in different sectors of the cyber space i.e. e-commerce, intellectual property (industrial property), Civil Liberty and Human Rights, and Cyber Crimes is different and limited.

3.3.1 CONVENTIONS ON CYBER LAWS

(CIVIL ISSUES)

Long series of Conventions were held in the US, Europe and United Nations since 1960s onwards to discuss and decide various items of electronic transactions. These included the legal value of electronic records in the eye of different municipal Law, the standard form, mode and validity of electronic contract, discharge of contract, specific performance of contract protection of copy right’ international trade and transactions, banking activities, and record keeping and like others.

The classical concepts as to creation custody and delivery of documents, enforcement of contracts, place of contracts, protection of intellectual property rights, authentication or signature, document, original, and duplicate etc. became very much confused in the e-media and could be decided or applied thereto.

So discussions conventions and experimental applications of new legal rules were required to cope with the new situation created by the e-media.

Series of Conventions were held in America, Europe and other countries involving regional governments, and commercial sector and it continued all through the 2nd half of 20th century till date. This age is said to be the third wave of legislation to manage and guide the market forces in the new e-media.

64* Sup -----3c ------- 1996--------P-------107
65* Sup -----1 ------- 1999--------P-------26
Alvin Toffler in his book, 'The Third Wave' observed that the early agricultural economy needed ownership protection for land and the products. And this led to the increased legislative activities as the 1st wave. And in the next phase the manufacturing and industrial production created another wave of legislation relating to production and circulation of capital, capital goods and manpower. 'In the Third Wave we have now entered, information to a large extent replaces land, capital, and hardware and .......... information is most at home in a much more fluid and adoptable environment'.

The information age has made a fundamental change in the mode of human interaction with others i.e. borderless media with free access and also in the concept of government. And a fresh attempt to make appropriate legislative framework has become necessary as a new wave of legislation on cyber space.

It is said that Information and Communication Technology (ICT) had started with the invention of electric telegraph in 1835 by Samuel Morse. So in a sense the first Cyber legislation may be traced to British Telegraph Act - 1868 .......... Then came the wireless telegraph and the relevant Act in early 20th Century. In India 1st telephone line was installed in 1875 and the Indian Telegraph Act - 1876 was enforced accordingly. In these cases also the transactions involving telegraph – telephone lines and wireless as a medium – the confusion as to rule of contract, violations and jurisdiction etc. arose as usual. And these had been addressed through series of conventions treaties and agreements at national and international levels. And the process of serious thinking and making one or other legal frameworks suitable for the electronic communication media also started in 1960s.

3.3.1 (a) TRADE AND COMMERCE

Trade and Commerce Sector first addressed the issues arising out of the telecommunication with electronic systems in the 1st half of the 20th Century and continued through the 1950s and 1960s. But with the advent of – electronic computer – and storage, processing and record making, electronic data interchange (EDI) through computer networks demanded a renewed look to the rules in this sector.

UNITED NATIONS:

It has been observed by UN General Assembly in its’85th plenary meeting held on 16th Dec. 1996. “Recalling its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law with a mandate to further the progressive harmonization and unification of the law of international trade.
Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication commonly referred to as 'electronic commerce' which involve the use of alternatives to paper – based methods of communication and storage of information". * 67 The legal value of electronic records, processing personal data, EDI through communication network and questions relating to transactions became the central issues in trade and commerce. And the UN Commission in 1995 further clarified its position on these issues for general use by concerned people. "Recalling the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session in 1985 ........ in which the Assembly called upon Government and international organizations to take action, where appropriate in conformity with the recommendation of the commission (1) so as to ensure legal security in the context of widest possible use of automated data-processing in international trade". * 68 And the UN convention held in 1980 on 'Contracts for the International Sale of goods' provided for the rules on electronic contract. And 'writing' in this connection was described to include any mode of communication preserving a record of the information contained therein and also being capable to be reproduced in tangible form (Article – 1.10), thus in addition to telegram and telex 'writing' in business transaction was interpreted to be an electronic record also.

COUNCIL OF EUROPE :- Council of Europe also held a convention in 1981 January for the protection of individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108). This convention provided for the cyber – rules dealing with information processing, privacy of individuals and free flow of electronic data among member countries.

TURKU – CONFERENCE :-

A broad based Conference on Global Electronic Commerce and related legal issues was held in Turku, Finland in November 1997. This Conference was attended by OECD member states (29 nations), Finland, Japan, through both government and business representatives. The conference worked on consensus based policy framework and also as to the guiding principles on electronic commerce.*68a

E C DIRECTIVE :-

The European Commission prepared a Directive for Cyber Legislation in September 1990 as a general guidance for European Community members including UK. In 1997 the European Commission adopted 'A European Initiative on Electronic Commerce' with the objective to create a favorable regulatory framework for electronic commerce. The commission in November 1998 made a
proposal on legal aspects of e-commerce and selected five areas to have common rules on the subject. These were (1) establishment of Information Society service providers (2) commercial communications (3) Electronic contracts (4) Liability of service providers (5) Implementations through uniform codes, co-operation and cross-border dispute management system.

**OECD:**

The Organization for Economic Co-operation and Development (OECD) – http://www.oecd.org with its 29 member states is a research group at Paris working on social and economic policies. The OECD participated in Turku (Finland) Conference (Nov. 1997) to frame policy and guidelines for electronic commerce.

**ICC:**

The International Chamber of Commerce (ICC) prepared a set of norms rules and concepts in 1999 on electronic commerce for general use. This text is known as General Usage for International Digitally Ensured Commerce (GUIDEC). This text provide for rules, norms and standards on different issues an authenticity of electronic message technologically reliable information system, ensured message etc.

*The International Institute for the Unification of Private Law (Unidroit) is based in Rome. Unidroit has framed a balanced set of rules in 1994 to be applied throughout the world in the areas of international commercial transactions.

3.3.1(b) **UN – WGIG – WORLD SUMMIT – WSIS:**

The UN Working Group on Internet Governance (WGIG) was set up under the mandate prepared in the 1st phase of the World Summit on the Information Society (WSIS) held in Geneva on 10-12 December 2003. The WGIG is now preparing for the 2nd summit (WSIS) to be held in Tunis in November 2005. “The WGIG has been asked, inter alia, to investigate and make proposals for action as appropriate, on the governance of the Internet by 2005”, dealing with the following issues.

- Develop a working definition of Internet governance
- Identify the public policy issues that are relevant to Internet governance.
- Develop a common understanding of the respective roles and responsibilities of Governments, existing international organizations and other forums, as well as the private sector and civil society in both developing and developed countries”. *69*

The UN WGIG working under WSIS mandate-analyses........

69* Report pf WGIG – June 2005 ........
http://www.wgig.org/- Download – 08-09-05 P – 3 Para – 5
existing state of affairs to prepare the working definition - "the WGIG analyzed a wide range of public sector, private sector and multi stakeholder governance mechanism that currently exists with respect to different Internet issues and functions". * 69A This WGIG has prepared the definition of Internet Governance for WSIS as follows "Internet governance is the development and application by Governments, the private sector and civil society in their respective roles, of shared principles, norms rules decision making procedures and programmes that shape the evolution of and use of the Internet". This working definition reinforces the concept of inclusiveness of Governments the private sector and civil society in the mechanism of Internet Governance". * 69B The WGIG also dealt with public policy-issues relating to Internet governance and also on the question of adequacy of existing governance arrangements. In the Plan of Action the UN - WGIG established four basic areas of public policy. These are (a) issues relating to infrastructure and the management of critical Internet resources, including administration of domain name system and Internet Protocol addresses (IP addresses), technical standards etc.

"These issues are matters of direct relevance to Internet governance and fall within the ambit of existing organizations with responsibility for these matters". And (b) "Issues relating to the use of the Internet, including spam, network security and cyber crime while these issues are directly related to Internet governance, the nature of global co-operation required is not well defined". (www.intgovweb.org) The other issues are relating to (c) intellectual property rights and (d) relating to the developmental aspect of Internet governance in developing countries.

INTERNET GOVERNANCE PROJECT :

The IGP is a consortium of academics, carries on study and research work on various issues on the Internet – like administration, autonomy, civil liberties and human rights in cyber space – and recently organized a world wide debate against the US intervention (August 2005) in the autonomous activities of ICANN as to domain name registration. Ref - infra '116' - F. N. - also - [http://dec.syr.edu/igp . home.htm] download 08-09-05.

UN - ICT Task Force - Report - 2004 :

The report observed that the “policy authority for Internet related public policy issues is the sovereign right of the states - Intergovernmental organizations have had and should continue to have a facilitating role in the co-ordination of Internet related public policy issues-------” * Ref. : infra 117 also - [http://www.unicettaskforce.org] - download on 08-09-05 – P - 1 – Para - 49

69A* Sup -----69 ------- 2005
69B* Sup -----69 ------- 2005
3.3.1 (c) INTELLECTUAL PROPERTY

In the area of Intellectual Property also the e-legislation has been a vital issue, specially in the matter of Copy Right and Trade Marks. The first series of conventions namely, the Paris Convention on Industrial Property (1853), the Madrid Agreement on Trade Marks (1886), the Hague Agreement on Industrial Design (1925) had provided for the protection of industrial knowhow, good - will and design, and also the commercially valuable creative works of individual work in art and literature. But in the new digital era – the necessary modifications were done in the 2nd half of 20th Century – such as the Berne Convention (1886) was revised in 1971 to accommodate computer program. The Rome Convention (1961) and the Geneva Convention (1971) provided for the phonograms & performers’ creative arts.

The World Intellectual Property Organization (WIPO) formed in 1967 came under the umbrella of UN in 1974. This WIPO organized copy right treaty (WCT) in 1996 recognizing computer programs as IP “with the ‘products’ in ‘electronic’ commerce in digital form, the – protection of such ‘products’ through intellectual property right become important. Traditional legal principles such as those in copyright law may be inadequate to cope with the digital – medium”. * 69C The General Agreement on Tariff and Trade (GATT) was signed on 1st January 1948 – and it included IP as a subject in 1986. And this body under GATT organized TRIPS Agreement (Trade Related Aspects of Intellectual Property) in 1994 to provide more or less uniform protection of IP rights in different member countries. Case : U.S – Vs – Hsu ( 3rd Cir ) 1998 – On disclosure of trade secret.

The European Community observed in 1995 through a report on ‘Copy right and related Rights in the Information Society – that harmonization of IPR laws only could protect the authors and concerned parties. The WIPO recognized and adopted the observations of the EC made in the above report (green paper) in December 1996. The WIPO Conference in 1996 considered and accepted two separate treaties – one concerning ‘Copy right in digital medium’ and the other on ‘the protection of performance and protected the computer program in any form as literary works of the programmer. The Global Information Infrastructure Commission (GIIC) also strongly recommended for Harmonization of IPR laws to have any effective legal control on IPR violations in cyber space. One T.M. related Case : - Inset Systems – Vs – Instruction Set – 937 F . Supp . 161. D.Conn.1996.

69C* Sup – 5 ---------------- P – 176 ---------------------- 2001
3.3.2- ISSUES ON CYBER CRIME:

Cyber space and Internet were mainly the subject matter of research and experiment in the 1970s and 1980s. And full range of Internet was not available to common people before 1984. only e-mail facilities were enjoyed by the people in 1980s in USA and Europe. But crime in cyber space appeared much late in 1980s first in telecommunication network ( like Kevin Mitnick.....) then through Internet. The phone hackers called phreaks, applied their expertise knowledge and perseverance in breaking into the cyber space mostly unguarded then “cyber crime has only recently begun to receive the attention that this massive problem warrants. The shift of crime to intangibles has a staggering impact on society, both socially and economically”.*70. And very soon new items of offences like virus, worms, spamming, stalking, and so many others become regular feature in the cyber-space. The offenders like joy-walkers freely moved about the space beyond the reach and knowledge of all concerned “where terms like cyber tort & cyber fraud and ‘cyber terrorism’ originate, the stimulus for regulation is created ...... and that the potential of traditional legal tools to solve multi jurisdictional conflicts must be fully investigated. *71. Internet in 1980s was used for e-mails, communications among research groups regarding experiment on cyber-space and other subjects. The necessary, social political and legal atmosphere to fight cyber crime and hence serious thinking on cyber crime was started only in late 1980s and 1990s.

The Law enforcing agencies, (LEA) the social workers groups, civil liberties associations and legal communities took initiatives to hold seminars, discussions conferences and convention and also to draft legal texts and to create suitable legal and administrative frame work in the subject.

3.3.2.a – CONVENTIONS ON CYBER CRIME

A suitable balance between civil rights and administrative interference has become a serious issue at international level. To curb the crime without infringing privacy rights of citizens i.e. not to be exposed to unreasonable search and seizure, has been an important issue to civil liberty.

AIDP – 1992

The Association International de Droit Ponal (AIDP) has been engaged in the study of crime on the Internet. In 1992 October the AIDP organized a conference on cyber crime at Wartzburg, Germany “the AIDP released its report on computer crime at the conference... the report stated that less than five per cent of computer crime was being reported to law enforcement authorities”. *72

70* Sup-6------2001---p-215
71* Sup-1------1999---p-318
72* Sup-5------2001---p-523
High level international effort on cyber-crime had been taken by Council of Europe, European Union (EU) and G-8 countries, OECD and United Nations.

**COE-CONVENTION – 2001**

The Council of Europe for the first time held a convention on cyber-crime in 2001 (NOV.8 to Nov.23) when twenty six out of forty three member stated attended and signed the convention. The United States, Canada and Japan were also represented as non member participants. This convention dealt with the concept and types of cyber crimes. The convention provided nine categories of such offenses such as eight property crimes-illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud child pornography and one non property crime such as copyright infringement and related offenses. Also the COE dealt with the question of dual criminality and took a liberal view favouring the victim country to define a particular computer crime in her own way. And at the same time the victim country can seek co-operation as to investigation from the other country. “Specifically, the convention requires that the country from where the crime originates, must, at the request of the harmed country, preserve and disclose data to the requesting party”. *73* The convention however left the jurisdiction issue to be decided by the state parties involved in a particular Internet crime.

**UNITED NATIONS:**

The United Nations in 1994 published a Manual on the prevention and control of computer-related crime, as a general guideline to member nations. The UN Manual advocated for concerted effort to build co-operation to harmonize legal procedures, to define computer crime. Again the UN in 2002 published thirteen Recommendations through its’ Information Security Permanent Monitoring Panel (ISPMP) (established in 2001). The expert body of PMP observed that “The vulnerability of global and national information infrastructures give birth to new challenges to national and international security, business activity and human rights. The problem of information security will not be resolved by the efforts of just one state or a group of states or on a regional basis. The solution of this problem demands a united effort of the entire international community”. *74* The UN through the Panel Recommendations addressed the issue of the protection of the Cyber Space from the criminal abuse by any quarter. And the PMP stressed for comprehensive consensus on the Law of Cyberspace, harmonization of different national cyber crime laws as far as practicable, and a systematic co-operation and mutual assistance at all levels. In this context, the UN duly recognized the legal materials already developed by COE Convention on Cyber Crime (2001 – NOV) and other responsible works at international and national level.

---

74* Sup-73-V-1------2005-p-243
The PMP of UN advocated for the creation of one Information Technology Agency at international level to frame rules on technical issues as protocols, ultra high bandwidth, inter operability of ICT management process and technologies, computer emergency response system at global level, sharing cyber-tracking information and technologies, academic program to promote awareness on cyberspace offenses, to stress on security management with due diligence and accountability for all responsible officers connected to ICT in both government and private bodies. The PMP also recommended for the due certification of all hardware firmware and software. And also observed that, “International law enforcement organizations should assume a stronger role in the international promotion of cyber crime issues. The competences and functions of Interpol and in the European context, Euro pol, should be substantially strengthened, including by examining their investigative options”.

The PMP also called upon the international scientific community including the World Federation of Scientists to propagate ICT in developing and backward countries.

**INTERPOL:**

The International Criminal Police Organization (Interpol) was established in 1923 having headquarter at Lyon, France. At present the Interpol has a global network through about 179 member countries and many intergovernmental and other criminal police authorities. The Interpol runs one office named National Central Bureau (NCB) in each capital (generally) of its member countries. Interpol maintains a round the clock, 24 hour/7 day a week, point of contact network to assist trans border investigation in ICT crimes.

**SEOUL – CONFERENCE – 2002:**

The Interpol organized a high-level Conference on Cyber Crime at Seoul in October 2002. The conference observed that greater co-operation among member and non-member states were required to effectively face cyber crime. “They shared a sense of hopelessness rather than of purpose. Over two thirds of Interpol’s member countries did not have any type of Cyber-laws. Most of the 50 odd countries which did have some sort of laws are known to be erratic in their enactment, limp in their implementation. with a common denominator being a certain lack of foresight about how crime games would evolve on the Internet”. The Interpol having its H. Q. in Lyon, France maintains close network among 179 member Countries out of which only 37 member states were represented in the conference. The Interpol has prepared manuals on cyber crime as a general guidance for law enforcing authorities at international level.

75* Sup-73 --- V-1---2005-----p-246
EUROPOL:

The European Union has established on February 2, 1992, another body named European Police Office (Europol), H.Q. in Hague, Netherlands. The Europol became fully active on and from July 1, 1999 to address cyber crime issues with the help of EU member states. Europol National Units (ENUs) established in member-states started to conduct joint investigations since November 2000. The Europol convention has framed rules and procedures to conduct such united action to face cyber-crime incidents.

COE – PROTOCOL (ADDITIONAL) – 2003 January 28:

The Additional Protocol to the Council of Europe Cyber Crime convention was agreed upon by member states on 28 January, 2003. The meet at Strasbourg included hate speech & publication through cyberspace as a form of cyber crime. “The purpose of this protocol is to supplement, as between the parties to the protocol, the provisions of the Convention on Cyber crime, opened for signature in Budapest on 23 November 2001 ..... as regards the criminalization of acts of a racist and xenophobic nature committed through computer systems”.

ICP L:

The International 16th Congress on Penal Law (ICPL) made a set of recommendations on procedural law in cyber space. The congress was held in September 1994 at Reo de Zeniero. The 16th Congress stressed for clarification on the ‘power of search and seizure’, scope of interception and legal value of such intercepted materials.

OECD:

“The first international effort in harmonizing the legal responses towards cyber-crime was appointment of an expert committee by the Organization for Economic Co-operation and Development, in 1983 in Paris to discuss computer related crime and the need for changes in the Penal Codes of the member countries”. The OECD text provided nine principles for the information security in cyberspace. The OECD principles provided for accountability and responsibility of all concerned with the information system like the owner, the user and the service providers. In 1986 the OECD prepared another report on criminal substantive law, jurisdiction problem, double criminality, law of extradition, mutual co-operation among different countries on cyber crime, evidence of cyber crime, effect of foreign judgments, network search in other countries etc.

77 * Supra – 34------- Edn. – 2005 ------ P - 945
78 * Supra – 34 ------- Edn. – 2005 ------ P – 222
The OECD also prepared a detailed guideline for member countries on cryptography in cyberspace which has been linked with cyber crime management. The OECD policy attempted a balanced control on the use of cryptography by the user and law enforcement agencies and allowed a limited freedom to the user, however, in this respect.

**OECD – 2004 – WORKSHOP:**

The OECD organized workshop on ‘spam’ in February 2004 (Brussels) and in September 2004 in Busan, Korea. The Workshop dealt with best practices and technical devices to control spamming in Cyberspace.

**UNITED NATIONS:**


**G – 8 – RECOMMENDATIONS:** 1995 & 2002

The group of eight advanced countries (G-8) prepared and published a set of 40 recommendations for legal and technical control of globally organized cyber crimes, in 1995 and also in 2002. “The Committees main objective was to establish a comprehensive set of principles which could give guidance to national legislation…..” *79

**G – 7 – EXPERT REPORT:** 1997 The group of seven advanced countries together with UK, Russia, European Union countries (G-7) set up one Expert Group (p8) in 1996 on the subject ‘Misuse of International Data Networks’. The P → 8 group of technical and legal experts prepared a report in December 1997. The report dealt with illegal and harmful activities in the Internet and also the transfer of illegal information to the users. And the expert group recommendations led to the establishment of a round the clock –24 hours seven day active network of expert technicians for cyber-investigation. This Expert Network is used by other non-member countries at international level also.

**STANFORD CONFERENCE:** 1999: An unofficial conference on computer crime (CISAC) was held in 1999 at the Stanford University, US. The assembly advocated for the adoption of criminal liability standard as would be suitable to concerned quarters. However they high
lighted some acts as offenses i.e. illegal entry into a computer system, disrupting computer system functioning, manipulating data to cause 'substantial damage' to persons & property, disturbing security measures, manufacturing or distributing tools to commit crime, applying Internet technology (ICT) to commit any act declared illegal by treaties (specified) and to commit any such offense with the intention to damage national infrastructure. TheC I S A C – Stanford University – US conference in 1999 also prepared a legal text on cyber crime with suggestion recommendations and rules.

COUNCIL OF EUROPE ± EXERT DRAFT – 2000

The Council of Europe through its European Committee on Crime Problem (CDPC) and Committee of Experts on Crime in Cyber – space (PC-CY) prepared and published on 25th April 2000 an elaborate description of legal frame work at national and international level (draft convention). The draft addressed the issue on transborder search and seizure, domestic criminal law and attempted to reach a common definition on different items of cyber crime such as illegal access, illegal interception, illegal devices, forgery & fraud in cyber-law, child pornography, copy right in cyber space. The text also dealt with the cases of attempt, aiding abetting, corporate liability, sanctions. The text in addition to substantive law, also dealt with procedural law relating to search and seizure of stored computer data (A/14), preservation and production of stored data, (Article – 15 &16) preservation and disclosure of traffic data, Article (17) and Jurisdiction (A/19).

The draft also addressed the issue of international co-operation through extradition (A/20,21,22,23) accessing and preservation of stored data (A/26,24,27) disclosure of traffic data (A/25). For the purposes of immediate follow up of crime incident the text provided for a special 24/7 network having point of contact in each member country. “Each party shall designate a point of contact available on a 24 hour 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of the investigation ...... such assistance shall include facilitating of, if permitted by the domestic law and practice, directly carrying out; 1-providing technical advices, 2- preservation of data pursuant to Articles 24 and 25; and 3- the collection of evidence, giving of legal information and locating of suspect". * 80

IIA:

The Internet Industry Association (www.iia.net.au) developed in May 2002 a detailed code of practice for better management of cyber law and order situation preferring free flow and use of cyber resources to greater restriction on the user community.

80* Sup-5----2001----p-491
The IIA code addressed the issue of ISP obligations and also on technical protection against intrusion by hackers and provided a list of standard filter products for general use like Content Keeper. Eye guard, Smart Filter, X-Stop, X-Stop - R 2000 etc. The Internet Industry Association (IIA) also developed a code for practical use in cyber crime management “The Internet Industry Association (IIA) and Law Enforcement Agencies (LEAs) recognize a commonality of interest between industry and government in prevention, detection and investigation of online fraud and other criminal activity and threats to national security and information infrastructure generally”.

The code addressed the issues like privacy, ISP obligation as record keepers, of operational data like data & time login and log out of a customer, CND or CLI where collected and other data like proxy logs (IP Address, Time, URL), e-mail Arrival, delivery, sender, recipient, size, newsgroup logs, FTP logs etc.

The code also addressed the issue that ISP can’t actually verify the identity of a person using a customer’s log-in in details and it also provided a set of the minimum period of retention for different types of data. Such as 12 months for personal data, 6 months for operational data, 1 week for other data. The code provided in details the rights and duties as between the ISP and LEAS and also on co-operation and exchange of information or disclosure by ISP. The code also dealt with the issue of security in cyber space and provided for ISP liability to cooperate with LEAs and to follow IETF guideline for collection and preservation, and disclosure of electronic data to the LEAs. The ISPs are also hereby called upon to report every incidence of criminal activities as and when it comes to its knowledge, to appropriate forums.

IETF:-

The Internet Engineering Task Force (IETF) drafted and published in November 2001 a set of “Guidelines for Evidence Collection and Archiving”. The procedural legal code of IETF has dealt with the violation or breach of security policy (called Security Incident) in any system or network. The system administrators (Sysadmins) are asked to follow these guidelines for security management and evidence collection.

UN - WIG - WORLD SUMMIT - WSIS:

The 1st World Summit on the Information Society (WSIS) held in Geneva (10-12 December 2003) established the UN - Working group on Internet Governance. And WIG is now preparing for the next Summit in Tunis in November 2005. The WIG is working on various issues like “Develop a working definition of Internet Governance - public policy issues that are relevant to Internet governance”.

Download
08-09-05: The Tunis Summit (WSIS) has been addressed by UN Secretary General Mr. Kofi Annan on 16th November 2005. “Under the deal, an international forum, under UN auspices, will be set up to examine Net issues. But day today management of the Internet will remain with the California based Internet Corporation for Assigned Names and Numbers (ICANN), a part private, part public body that reports to the Department of Commerce in Washington. The new forum will handle such cross-border problems as web viruses, cyber crime and spam. Rupert Cornwell – Washington – The Independent”. * 82


The UN – Information and Communication Technology Task Force Report has dealt with the rights of different sovereign states as to the policy of the Internet and also recognized the important role of the Intergovernmental bodies, NGOs and civil society groups. Ref: – FN – infra 106- [http://www.unicttaskforce.org]

3.3.2.(b) – SURVEY REPORT

The American Bar Association in 1987 had made a survey of computer related crime. They observed that about seventy two out of three hundred corporate and government agencies were victim of cyber crime and experienced loss of millions of dollars within preceding twelve months only.* 83 Another survey made in 1991 throughout US, Canada and Europe revealed that seventy two percent of the parties had been victim of cyber crime in some form. The A I D I P survey in October 1992 pointed out another point that “less than five percent of computer crime was being reported to law enforcement authorities”. * 84 It is thought that the reason of this dark figure might be the fear of losing the goodwill of a corporate body. The under reporting may be caused by some other factors like difficulty to detect the crime, or security incident (breach of security rules). Hence many cases go unnoticed beyond the knowledge of sysadmins (system-administrator). A very recent survey made at the beginning of 21st century by the UN revealed many notable points as to the nature of cyber crime and the management thereof. Most of the countries have recognized the criminal liability in the cases of unauthorized access. Computer related fraud, forgery, child pornography but not in the case of online gambling. “Countries are moving to adopt consensus crimes in certain areas ………. Significant progress has been made toward achieving consensus with regard to outlawing cyber crime against property and there is also a solid and growing, consensus on outlawing …… child pornography”. * 85

82* The Statesman – Kolkata --- 17.11.05 - --- P -- 2
83* Sup – 5----- Edn. 2001 -------- P – 522
84* Sup – 5----- Edn. 2001 -------- P – 523
But it is observed that legal provision as to child and child pornography are not uniform and lack precise definition in many countries. The age of a child has been recognized differently in different countries such as 14 years in Germany, 16 years in Norway, 18 Yrs. in Srilanka but undefined in France, Finland and Iceland.

3.3.2.(c) SECURITY GUIDELINES

On the subject of information security numerous materials in the form of suggestions, experiences and analysis have been drafted and published at international level. The collection of Best Practices in this subject has been popular and effective through the publication by different bodies working in this area. The Information Technology Infrastructure Library (ITIL) an autonomous body, stationed in UK prepared the ITIL Security World a literature on cyber security. Similar technological literatures have been drafted and published by some other bodies such as The Information Systems Audit and Control Association (ISACA) published COBIT (The Control Objectives for Information Technology guidelines). (2) One website CASPR (The Commonly Accepted Security Practices and Recommendations) prepared and published in 2002 a set of best and tested practices on information security. A professional training association SANS (the Systems and Network Security Institute) has published literatures prepared the basis for developing security norms and legal provisions in cyber space. The Best Practices with suggestions and experiences are further concretized into ‘standard practices’ by different professional groups and responsible associations, like International Standards Organization (ISO), International Telecommunications Union (ITU) and different national bodies like British Standards Institute, European Telecommunications Standardizations Institute (ETSI). National Institute of Standards and Technology of USA etc. The other such bodies are also active in this subject such as N A T O (for Orange and Red books of 1980s).

Many other expert groups and associations like IETF, IIA, are actively engaged in formulating security standards and norms. The corporate bodies in the private sector are also preparing and developing security norms and standards for the purposes of crime management. Some of these initiatives are referred to International Chamber of Commerce (ICC), The Global Business Dialogue on Electronic Commerce (GBDE), the Global Internet Project (GIP), the Global Information Infrastructure Commission (GIIC). The autonomous civil liberty and human rights groups, associations are also active in formulating drafting and publishing legal materials in the form of suggestion, and models. The Electronic Frontier Foundation under chairmanship of Esther Dyson published semi-legal literature ‘The code of conduct’*86 The text dealt with ‘guidelines for net users or Netiquette, ways to fight junk mail, civil liberties in cyberspace, ways to stay virus-free, how to avoid on-line hoax, etc

86* Sup-3c---1996---p-115
Some relevant literature on privacy rights were published in 1994 by Winn Schwartau (http: II www.web crunchers com/cruch) under the title ‘Electronic Bill of Rights. “The six point Electronic Bill of Rights takes in to account the realities of modern technology and over arching legislative wisdom ....... These simple principles will bring back much of the privacy that has been eroded away since the dawn of the computer age". * 87 Such text materials supply the essential ingredients, limits and potentials of actual cyber legislations. In a case: Janet Reno V ACLU (American Civil Liberties Union) (1997 US) the right to speech and expression was upheld by the Court as against the order of injunction under Communications Decency Act 1996 on running an adult Website by J.Reno. The Judicial observations, ratio decideni and obitur dicta on Internet related proceedings are also providing valuable materials on cyber legislations being made by all legislatures.

In the subject of ethical rules – Richard Mason in 1986 identified four areas – (Privacy Accuracy, Property and Accessibility (PAPA) as to cyber space code of conduct. "Organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN), Civil Society Internet Forum and Computer Professionals for Social Responsibility (CPSR) have formulated various recommendations and guidelines that seek to regulate the impact of Web technology on society." * 88 The Computer Ethics Institute (CEI) thus prepared and published ten rules (Ten Commandments of Computer Ethics) – Such as 'Thou shall not Use a Computer to harm other people, not to interfere with other peoples' computer work, not to snoop around in other peoples computer files, not to use a computer to steal, not to use a computer to bear false witness, not to copy or use Proprietary Software for which you have not paid, not to use other peoples computer resources, not to appropriate other people’s intellectual output, shall think about the Social Consequences of the program you are writing or the system you are designing, always use a computer in ways that ensure consideration and respect for your fellow humans.

Similarly the Software Engineering Code of Ethics and professional practice by Software Professionals were drafted published for general guidance for the user community as well as the legal drafting.

88* Sup --45 ------- Edn. – 2003 ------- P – 7
3.3.3. CYBER LEGISLATIONS

In traditional concept 'governance' means, 'to rule with authority'. But in cyber space 'authority' is missing as none can assert authority over the whole cyberspace. This vacuum is some how managed by inter national agreements and understanding at various levels for mutual assistance, and co-operation. But governance of a kind is needed in civil and criminal issues and also in administration and technical management of the Internet. Throughout the ages, any and every governance has been dependent on some kind of practices standards and norms, which may or may not be codified. Mainly from 1970 onwards, different necessary and suitable standards, norms rules and specific statutory provisions are being developed on different subjects of cyber-space. The different areas requiring rules and legal provisions are administrative and technical management, such as protocol selection, space allocation, network registration, IP address and domain name distribution and management etc. The other areas are e-Commerce, intellectual property rights in cyber-space and the fourth is the cyber-crime.

In e-commerce country wide specific legislations like Data-Protection Act 1984 of UK and the like have been framed on recognition and management of electronic data at national and regional level. But cyber-space being undivided and global phenomenon the country-wise laws needed to be supplemented by many international agreements treaties conventions and covenants organized by different concerned international level bodies on the subject like O E C D (organization for Economic Co-operation and Development) ICC, Council of Europe, European Commission.

3.3.3.(a) RULES ON CIVIL ISSUES (OPERATIONAL MANAGEMENT)

At present the functional or operational management of the cyber space is done centrally by non-profit autonomous bodies but not through the positive laws as such but through a new mode i.e. creation and adoption of standards, and then concretizing them gradually into norms and rules. In the first era of the Internet (i.e. 1969-1985) the network wide operational management was in the hand of the I P T O (Information Processing Technique Office) of A R P A. This I P T O for the first time took the task of standard setting in the network and developed Transmission control protocol (TCP) and Internet Protocol(IP) for general use by network community. "The participants in the Internet Communicate by using a common protocol. What lays behind the success of the Internet TCP/IP is the principle of "open standards". That means the protocol is first written, then freely distributed to anyone who wants to use it. Overtime, the protocol is revised, building upon the experiences of the users and not just the original authors". *89
This code language TCP/IP was not enforced as a binding rule but left to be used by
the user community as an open standard. And on 1st January 1983 this code TCP/IP was
accepted uniformly as a more concrete norm for all networks connected to the Internet
backbone. This standard setting and norms creating process was conducted centrally for
operational convenience. This mode of network wide operational management through non­
binding soft law has been gradually recognized accepted and applied by other autonomous
bodies like ICANN, ISOC, Inter-NIC, w3c etc.

The Internet Society (ISOC) (http:www.isoc.org) established in 1992 co-ordinates
various technical management issues and activities done by I E S G (Internet Engineering
Steering Group) IETF (Internet Engineering Task Force). "The Internet Society (ISOC) is
the most comprehensive of the new Internet Organizations. ISOC is a non-profit professional
society founded in 1992. It organizes information events and working groups and co­
ordinates some of the efforts of other Internet administrative bodies. Standards and protocols
of the Internet are developed primarily by the Internet Engineering task Force (IETF), which
is an open international body mostly composed of volunteers. The activities of the IETF are
coor-dinate by the Internet Engineering Steering Group (IESG) and the Internet Architecture
Board (IAB) which are affiliated with ISOC" 90

IETF :-

Thus in the area of operational management the ISOC and like bodies select or evolve best
practices and set standards and norms as part of cyber-law making process. "For the last 10
years the Internet Engineering Task Force (IETF) has been the main organization creating
standards for the Internet... The IETF tends to focus on infrastructure standards such as
TCP/IP, the web transport protocol http and the new differentiated services functions and
protocols used to transport voice and video across the Internet. http://www.ietf.org>" 91

NSI :-

Similarly the domain names of websites are distributed and registered by NSI
(Network Solutions Inc) and ICANN (Internet Corporation for Assigned Names and
Numbers) and also make relevant norms and standards and also decides disputes as to
website names and addresses. The growing problem relating to naming a website, conflict
with Trade Mark, under the NSI (Network solutions Inc.) led to further development of
official activity. "This initiative led to the incorporation of the Internet Corporation for
Assigned Names and Numbers (ICANN) in 1999

90 * Sup- --1---End---1999---p-55
91* Sup-----17-----2000-----p-269
a non-profit organization incorporated in California, US, ICANN has assumed responsibility for the central coordinating functions of the Internet such as IP address, space allocation, protocol parameter assignment, domain name system management and root server system management function. ICANN now requires its accredited domain name registrars to abide by various specifically stated procedures and consensus policies. This includes a uniform domain name dispute resolution policy applicable to all registrars.

ICANN:-(www.icann.org)

The administrative body NSI or ICANN on name registration thus frame rules and regulations (soft, non-binding) as a part of cyber-legislation in a new way. This is done like corporate body but with a non-profit cum public interest approach.

NIC:-
The NIC (Network Information Center) of the Internet, being one of Internet bodies also participate in distribution and allocation of domain names for websites. And at the same time takes active role in making rules and regulation as to the subject concerned (http://rs.internic.net/scout). Thus the rules and regulations so far administrative and technical management of the cyber space is concerned are framed by these Internet bodies on the basis of a non-profit motive.
The Rules are:-

A. The ICANN Uniform Domain Name Dispute Resolution Policy As approved by ICANN on 24th October 1999.

B. The Rules for Uniform Domain Name Dispute Resolution Policy (Approved by ICANN on 24th Oct, 1999).

* INTER GOVERNMENTAL FORUM – has been formed in the 2nd World Summit (November – 16th, 2005) held in Tunis to look after the cross border issues related to worm dropping, span and other cyber crimes Ref - CH 3.4.a

92*Sup—32—Edn—2001---p-6
The commercial sector first attempted to legislate on cyber transactions recognition of electronic data, messages, and electronic contracts. The issue comes through computer-telecommunication systems in 1960s and 1970s. So the trade law issue was taken up by the UN in 1966 in the Commission of Trade law on International Trade involving electronic communications. And Internet was opened to commercial use only in mid 1990s though e-mail service was available to a section of the people in the 1980s also. So in the pre-Internet period in 1960s, 1970s, and 1980s, the computer-aided telecommunications service and e-mail (Internet) facilities demanded new rules as to contract and related issues. And the UK framed the Data Protection Act-1988 in this period. CASE :- Henkel vs. Pape (1870) LR6 Ex.7 A number of Conventions were held to frame rules on international trade contracts involving computer-telecommunication system and e-mail facilities.

From mid 1990s the Commercial access to full range Internet was assured together with privatization of the backbone lines. And some private network backbone like UUNET, PSI were also made active in the U.S. And commercial activities rapidly grew in Internet which is called e-commerce. “Almost all of the commercial world-wide-web sites, estimated in 1998 at 2,50,000 have come into operation since the beginning of 1996. About 80% of these have monthly sales figures of less than US $ 10,000”. *93

The commercial transactions may be direct and indirect ones. The direct electronic commercial transactions may be on-line ordering, payment and delivery of intangible goods and services such as computer software, entertainment or information services.

The types of transactions in cyberspace range from informal personal correspondence to exchange of formal documentation and to transactions involving payments. Where transactions become commercial, the complexity increases as to the contract, parties to the contract, records of contract and related communications, enforcement and trials. “Like proposer and acceptor in the case of physical contract a new concept ‘originator’ and ‘Addressee’ has been recognized in the case of electronic contracts. This has become necessary because of the fact that most E-contract are executed between computers linked to a network.”. *94

The important issues such as time and place of Dispatch and Receipt, acknowledgement of receipts, recognition of electronic records etc. also have been decided upon to ensure electronic commercial activities.

UNCITRAL Model Law on Electronic Commerce-1998
Definitions :- Article2 (a) ‘Data message’ –

93 * Sup---1 - ---Edn. 1999---p-49
94 * Sup---32- ---Edn. 2001---p-30
Means information generated sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy:

Art. 2/b - Electronic data interchange (EDI) means the electronic transfer from computer to computer of information using an agreed standard to structure the information.

Art. 2/c - Originator of a data message means a person by whom or whose behalf the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

Art. 2/d - Addressee of a data message means a person who is intended by the originator to receive the data message but does not include a person acting as an intermediary with respect to that data message;

Art. 2/e - Intermediary with respect to a particular data message, means a person who, on behalf of another person sends, receives or stores that data message or provides other services with respect to that data message;

Art. 2/f - Information system means a system for generating, sending, receiving, storing or otherwise processing data message.

Article 5 - Legal recognition of data messages. Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Art. 6 - Writing - (1) where the law requires information to be in writing that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

Art. 7 - Signature - (1) where the law requires a signature of a person, that requirement is met in relation to a data message if;
(a) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances including any relevant agreement.

Art. 8 - Original - Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if;
(a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as a data message or otherwise, and
(b) Where it is required that information be presented that information is capable of being displayed to the person to whom it is to be presented.

Art. 9 - Admissibility and evidential weight of data messages.
Art. 10 – Retention of data messages – (1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages provided that the following conditions are satisfied:

(a) Information contained there in is accessible so as to be usable for subsequent references; and
(b) The data message is retained in the format in which it was generated sent or received or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
(c) Such information, if any is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

A.12 – Recognition by parties of data messages:

A. 14 – Acknowledgement of receipt – (2) Where the originator has not agreed with the addressee that the

acknowledgement be given in a particular form or by a particular method, or acknowledgement may be given by.

(a) any communication by the addressee, automated or otherwise, or
(b) any conduct of the addressee sufficient to indicate to the originator that the data message has been received.

Article – 15 – Time and Place of dispatch and receipt of data messages – (1) Unless otherwise agreed between the originator and the addressee the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) If the addressee has designated an information system for the purpose of receiving data messages, receipt occurs.
(i) At the time when the data message enters the designated information system; or
(ii) If the data message is sent to an information system of the addressee that is not the designated information system at the time when the data message is retrieved by the addressee;

(b) If the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
(3) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business;
For the purposes of this paragraph:

a) if the originator or the addressee has more than one place of business the place of business is that which has the closest relationship to the underlying transaction or where there is no underlying transaction the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

Art. 16 - Actions related to contracts of carriage of goods.

Art. 17 - Transport documents.

INDIA: -

On electronic commerce and related issues the Indian legislation is a draft bill – The Electronic Commerce Bill – 1998 – provides for similar provisions as -

S/6 - Legal Recognition of electronic data and messages
S/7 - Writing in electronic form
S/8 - Electronic Signatures
S/9 - Original Record
S/10 - Admissibility and Evidentiary Weight of Electronic Records and Electronic Signature
S/11 - Retention of Electronic Records-
S/12 - Secure Electronic Records
S/13 - Secure Electronic Signature
S/14 - Presumption Relating to Secure Electronic Records and Signatures
S/15 - Formation and Validity of Electronic Contracts
S/16 - Effectiveness between the parties
S/17 - Attribution of electronic record to the originator
S/18 - Acknowledgement of Receipt
S/19 - Time and Place of Dispatch and Receipt (Some Spirit as that of UNCITRAL – Article -15).
S/20 - Applicable Law – the dispute on contract to be decided on the basis of (a) the law designated by the parties (choice of law – rule); (b) in absence of any choice by the parties concerned – the court or arbitral tribunal shall apply the rules of law which appears to be appropriate with-reference to the surrounding circumstances of the dispute (c) the court also to take into account the terms of the contract in question and the usage connected to the trade concerned.
S/21 - Secure Electronic Record with-Digital Signature.
S/22 - Digital Signature as a Secure Electronic Signature.

The Information Technology Act –is the only law enforced on 17th October 2000 in India – covering electronic commerce and cyber crimes. This IT Act also relied upon the same and similar spirit and text of the previous Electronic Commerce Bill – 1998(India) – and provides for legal recognition of electronic data, data-message and contracts as follows-in brief---

S/3 – Authorization of Electronic record by affixing digital signature
S/4 – Legal Recognition of electronic records
S/5 - Legal Recognition of digital signature
S/7 - Retention of electronic records
S/11 - Attribution of electronic records to the originator
S/12 – Acknowledgement of Receipt
S/13 – Time and place of dispatch and receipt of electronic record.

In absence of any agreement between the originator and the addressee, (1) The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator. (2) The time of receipt of an electronic record shall be determined as follows namely –

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records:
   (i) receipt occurs at the time when the electronic record enters the designated computer resource, or
   (ii) if the electronic record is sent to the computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.

(3) the electronic record is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business.

(4) the provision under subsection (2) will apply even in the cases where the location of the receiving computer resource is different from the place where the electronic record is deemed to have received i.e. place of business.
For the purpose of the section –

(a) if the originator or the addressee has more than one place of business the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) 'usual place of residence' in relation to a body corporate, means the place where it is registered;

S/14 Secure Electronic record – where any security procedure has been applied to an electronic record at a specific point of time.

S/15-Provides for Secure digital signature – rules to make the digital signature unique for identifying the subscriber.

S/16- provides security procedure as prescribed by the Central Government for the protection of electronic records and digital signature.


Some other laws in this subject are –
UK Data Protection Act – 19084
Utah Digital Signature Act – 1995 (USA)
California Digital Signature Act – 1995 (USA)
German Digital Signature Law – 1997
Massachusetts Electronic Records and Signature Act – 1997
Federal Electronic Financial Services Efficiency Act – 1997 (Baker Bill)

3.3.3.C RULES ON DIGITAL I.P.

In the areas of Intellectual Property – the law in cyberspace is in a cross road due to widespread software piracy and different technological innovations (creating issues like MP3, Napster, Framing etc). The question of copy-right is really beyond any solution in present context. “What is to be done? While there is a certain grim fun to be had in it. dancing on the grave of copy-right and patent will solve little, especially when so few are willing to admit that the occupant of this grave is even deceased and are trying to uphold by force what can no longer be upheld by popular consent” *95 The Intellectual Property rule making started in 15th Century when the first glass making patent was granted in Italy. “The city Council of Florence awarded the first recorded patent or letters patent, in 1421 for

95* Sup-3c------------------------1996------------------------p-108(2)
the production of glass. This was the first of several patents granted in order to provide specific privileges in the fifteenth century in the small states of Northern Italy. *96. Managing IP-2002. In 1449 Henry VI of UK issued the Patent (first in England) for making a special variety of glass (stained glass). Through Judicial decisions the patent rule was gradually enriched. In USA the first patent rule was enforced in 1641, but first Patent Act was enforced in 1790 in US, then time to time modified such as in 1836-1870-1952. The Paris Convention on Industrial Property in 1883 initiated a further wave of legislation in different countries, and Japan framed patent law in 1885. And in 1970 Patent Co-operation Treaty (PCT) was concluded by WIPO. The UK passed Patent Act 1997 based on modern concepts.

In case of Copy Right protection, the statute of Anne-1709 was passed in UK to protect author’s right for the reason of the new printing technology in UK. The United states also passed similar law at that time. The Berne Convention -1886 (revised in 1971) provided for further legislations at global level. In 1893 the Bureau on Intellectual Property under Paris Convention – 1883 and the Bureau on Copy Right (under Berne Convention -1886) came together. This joint body continued and renamed World Intellectual Property Organization (WIPO) in 1970 which was again placed under UN in 1974. G A T T – agreement as revised in 1986 provided for copyright and related rights under section – 1 “Article 10-computer program and compilations of data......

1 – Computer programs, programs, whether in source or object code, shall, be protected as literary works under the Berne Convention (1971).

2 – Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such, such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself”. P-605./153. The protection period extended to 50 years U/a-12. And A/14 therein protected performances phonograms (sound recordings) and Broadcasting, the term of protection for phonograms and broadcasting was also for 50 years U/A-14 (5) of the G A T T (1986).

And in section 6 the provisions U/A-35 provided for the protection of Layout Designs (Topographic) of Integrated Circuits as per IP in respect of Integrated Circuit (IPIC) Treaty. The protection covered importing selling, or distributing for commercial purposes any protected lay-out design or integrated circuit chip containing the layout-design or any article containing the same IC-Chip. And the term has been extended to 10 years U/a 38 of the GATI (1986).

---

96* Chris Fitz simmon & Tim Jones – Managing Intellectual Property ---- Edn.2000---- Capstone Publishing Co- UK------p-16
Similarly the TRIPS agreement under WTO concluded in 1994 (effect 1 st January 1995) provided for digital IP also. The TRIPS provided for the same protection for computer program (U/A.10) for 50 yrs (A/12) and phonogram-sound recording (U/A-14) for 50 years A/14(5). The WTO-TRIPs also provided for the protection of Lay-out Designs (topographies) of integrated circuits U/A-35 and the term was for 10 years against import, sale or distribution U/A-38.


Some other legal provisions are found in The WIPO copyright Rules 1996. The WIPO performances and phonograms Treaty Rules 1996. I C A N N – Uniform Domain Name Dispute Resolution Policy-1999 etc.

In India – the British Copyright Act-1911 was taken as basis and then Copy Right Act 1914 was enforced in India. Again with the British Act-1957 India framed the Copy right Act 1957. The CR Act of 1957 covered changes due to technical advancements like communication, broadcasting microfilming and movies. In 1994 necessary amendments were made to the Copy right Act 1957 to give effect G A T T principles and the protection was extended to cover computer software and design layouts. The IP Law in India – is based on The Patent Act 1970, The copy right Act 1957. The Trade and Merchandise Mark Act 1958(The Trade Mark Act 1999), The Designs Act 1911 (The Industrial Designs Act 2000). And also that India has ratified Paris Convention – 1883 as amended and revised in 1967, 1998. The Semiconductor Integrated Circuits Layout Design draft bill provides for protection of
10 years for the author. And India being a party to the GATT-1948 as revised in 1986 has given effect to the concerned provisions relating to digital IP i.e. A/10 for computer program, A/14 for Phonogram and Broadcasting, A/35 for Layout Designs of IC chips etc. “consequent upon India signing the GATT and entering the global market economy, a number of changes have been made in the Copyright Act –1957 by the Amending Act of 1994 ... *98 The copyright Act –1957 as amended in 1994 provides for computer software and program (U/S 2ff(e)) and its protection. the IT Act does not provide for digital copyright and its protection however.

3.3.3.(d) LAWS –ON CIVIL LIBERTIES AND HUMAN RIGHTS IN CYBER SPACE

In the subject of Civil Liberties and Human Right- the issues of freedom of speech and expression, privacy, security of personal information resources- are facing a real crisis due to wide spread state intervention, surveillance and monitoring in the name of crime management. Effective legislation in these areas – up to a certain reasonable extent at least is not so easy because multiple jurisdiction problem and high-tech system. “The issues surrounding censorship of on-line communication are numerous and complex. Most stem from the question of jurisdiction, since the Net is the first truly global medium. *98A. The community standard of originator and addressee may be the law enforcing agencies to whom information is always valuable. But in the issue of civil liberty and human rights the privacy is priceless. The issue of interception by LEA & also raises serious objections by civil liberty activists. The GOI in ISP guideline provides that “Individuals/groups/Organizations are permitted to use encryption up to 40 bit key length in the RSA algorithms or its equivalent in other algorithms without having to obtain per mission” *98B. And this issue to restrict personal cryptography has been raised by law enforcement authorities. But this is certainly an attempt curbing privacy of personal or confidential communications. The issue of pornography and indecent communication also has been an issue as to the extent of legal control in private and intimate life of the man.

Case:- US V Thomas – 74 F.3d. 701 (6th cir 1996) A California website providing pornographic pictures was prosecuted in a Tennessee court by a resident of Tennessee where such materials are illegal. California law was not so strict. (p-523-R.D. Ryder). Thus the question of the definition of obscene material will be a confusion in law and practice. Case:- A C L U V Reno-1996 WL65464 (E.D.Pa) A pornographic website was sued by American Civil Liberties Union on the plea to protect tender minds of children and an injunction was allowed.

98 * Supra –97--Edn.--2002--p253
98A* Sup-3c---1996 ------P-30
98B* Supra –5--Edn.--2001--p716
3.3.4 - SCOPE OF LEGISLATION ON CYBER--CRIMES

In the issue of cyber crimes -- the scope of effective legislation becomes limited for the reason of easy anonymity involvement of multiple national Jurisdictions, standards of crime and also for rapid technological developments and innovations (Moore's Law -- processing power of IC chips doubles every 18 months by R & D) in Cyber System. “Perhaps as important, the non-corporeal nature of hacking has yet to be grasped and understood by both law enforcement and the mainstream media. As a result hackers are continually defined in corporeal terms in an effort to reattach the act of “hacking to a physical presence”. *99 This new mode of virtual crime does not fit to the traditional rule of criminality and criminal liability. As to the definition of crime the local values and concepts can't be ignored simply to make a uniform code. So the community standard poses another difficulty in defining crime and liability attached thereto.

The present form of cyber-governance is a two tier systems operating at national and International level the prevailing law enforcement agencies are acting mainly on the end users of the Internet with or without any cyber law in exercise of the national sovereign power “Controls can, of course, be implemented on end-user computers, For example, central information technology departments in large organizations can install software to prevent users from performing certain functions”*99A. At the international level -- different national governments are active to fight cyber-crime through mutual co-operation, law of extradition, information sharing, increasing technical assistance and hot-line communication, round the clock 24/7, Offices or Network Operation Centers (NOC) -- and Interpol “To a very large extent the evolution of international law has been influenced by the continuous shaping and modification of rules in response to changing international conditions. In this process international law is developing from an international law of co-existence to an international law of co-operation”. *100

The cyber space composed of the Internet and global communication network may give rise to a new phase of international law in near future. The Internet physical infrastructure, in most cases are under the care and control of the concerned territorial sovereign or sometimes any national body corporate. This care and control however remains limited only to the extent of keeping the transmission line in good repair and to update the system technically from time to time. This control, however does not extend to monitor the -- Internet traffic like telecommunication authorities. So, in true sense the burden of keeping the line active and efficient brings no benefit to the so-called authority so far governance is concerned.

99a* Sup ---17 -----2000 ------- P-------265
100* Sup ---1 ------1999-------- P-------26
In the issue of cyber governance its global reach, free access (access without prior permission unlike telecommunication system and absence of competent global authority or effective international agreement, legislation for cyber space at global level (cyber globe) could not be successful so long. The regulation or legal control in the interest of business-directly through a MNC like corporate body or through sovereign government also finds no strong ground to stand upon. And hence some of the technically advanced countries individually have been engaged to frame various laws on various aspects or issues like torts, e-contracts, digital – signature, pornography & obscene materials, intellectual property issues and offences like hacking. All these legislations are an experimental basis to fit the electronic space as far as possible.

Thus the Cyber Law, so far framed has many distinct limitations as to jurisdiction, enforceability, procedure and application – scope and extent. "We now face the task of adapting our legal institutions and societal expectations to the cultural phenomena that even now are springing up from communications technology". *101 Having failed to impose business interest regulation either directly through a body corporate or indirectly through a sovereign government the cyber legislation as of now is guided by public good, moral and social values and common sense rules.

3.3.4. (a) – LANS ON CYBER CRIMES

In spite of confusion on jurisdiction forum and enforcement, Laws on Cyber space are being enacted and enforced successfully at least to some extent. However it is not yet settled and clear to the legal community, how far the present form and style of legislation will be successful. So the scope of cyber law its reach and effectiveness are not, clear both in theory and practice. "As communication and data technology continues to change and develop at a pace many times that of society, the inevitable conflicts here begun to occur on the border between Cyber space and the physical world". *102 The present form of legislations aim to control the end users being the subjects of the concerned sovereign. As to the other nationals the cyber law depends on regional agreements conventions, covenants as to e-commerce, IP Law and like others.

101*Sup3C---1996---p-158
102*Sup3C---1996---p-14
The law of extradition through treaties and conventions are applied in the cases of cyber offenses involving multiple jurisdictions. Attempts are also being made to harmonize cyber laws including cyber-crime laws of different nation states. Round the clock (24 hours through 7 days) hotline contact centers and networks in each national territory are being set up to co-operate mutually to investigate cyber crimes. The substantive criminal law including definition of cyber crime, determination of criminal liability in cyberspace, the procedural law for investigation and trial, track and trace, detection, interceptions encryption search & seizure, evidence collection, preservation and production etc were required.

It was also understood that the harmonization of different legal systems at global level and global investigation network and mutual assistance at international level are also needed. And this multipurpose venture was taken up by the legal community throughout the world. Different regional and global organizations like COE, EC, OECD, UN, ICC etc. framed model laws and rules. And the national legislatures of different countries also passed laws, both substantive and procedural laws, to deal with this new form of crimes. The Council of Europe through its' select committee prepared a "Minimum list of cyber-crimes" in 1989. In 1992 the OECD prepared a guideline for the security of Information system. In 1995 the UN prepared and published a "Manual on the Prevention and Control of Computer Related Crime" and addressed the issues of substantive criminal law, procedural Law and international co-operation. Many national governments made necessary amendments in the existing criminal codes to face the growing problem of cyber crimes, and many others framed separate codes for this purpose.

The United States, the motherland of cyberspace, passed a good number of cyber laws on Criminal issue both at Federal and state level. Some of the US Federal legislations are :

1. Title 18 of US code: The Computer intrusions and other computer related crimes. The statute makes unauthorized access to a computer (or exceeding the limit of authorization) an offense. And it also defines specific crimes such as hacking cracking, virus, password trafficking etc.

2. Title 18 of US code :-
Unauthorized access to stored electronic communications – the statute also criminalize the unauthorized access or exceeding authorization.
3. Title 47 of US Code :-
The Child Online Protection Act (COPA). The statute makes it an offense to make available any harmful material to minor through cyber space. In reference to the ACLU Vs. Reno 217 F. 3d 162 (3d Cir, 2000) the statute has been kept under Judicial review in relation to the 1st Amendment.

4. 18 US code (1029) :-
On Fraud and Related Activity in connection with Access Devices.

5. 18 US Code (1030) :-
On Fraud and Related Activity in connection with computers.

6. 18 US Code (1362) :-
On Communication Lines, Stations or systems.

7. 18 US Code (2319) :-
On Criminal Infringement of a copyright

8. 18 US Code (2318) :-
On Trafficking in copies of computer programs, copies of motion pictures or other visual works.

9. 18 US Code (2319A) :- On Unauthorized fixation of an trafficking in sound recordings and music videos of live musical performances.

10. 18 US Code (1832) :- on ‘Theft of Trade Secrets’

11. 18 US Code (2261A) :- on ‘Interstate stalking’

12. 18 US Code (2510) :- on Interception of wire, oral and electronic communications.

13. 18 US Code (2701) :- on Preservation and disclosure of stored wire and electronic communications.


And some sentencing guidelines have also been framed for the cyber crime offenses. “It can be seen from the above list of provisions related to offences, their investigation and sentencing, that USA is one of the countries that
have achieved a lot of progress in combating cyber crime, in respect of legislative response”.  

103 The US state legislations also provided for various aspects of cyber crime such as definition, criminal liability in hacking, cracking, virus programs, pornography, cyber-stalking and harassment, cyber-fraud forgery and theft, gambling through Internet and also anti-government activities. Some of European, Asian and other national legislations are:

1. The Computer Misuse Act – 1990 (UK)
2. The Criminal Damage Act – 1991 (Ireland)  
(for computer / Computer System)
3. The Computer Crimes Act 1997 (Malaysia)
6. The Protection of Personal Data – 2000 (Austria) (the Privacy Act)
8. The Electronic Commerce Act – 2000 (Philippines)
10. The Electronic Commerce Act – 2001 (Malta) (includes Computer Misuse)
11. Amendments to the Criminal Code 2001 (Belgium)
13. The Electronic Commerce Bill ( 1998 ) ........ India

103*Supra – 34------------ Edn. – 2005 ------------- P - 122
Other than national legislations some regional bodies like COE, OECD, Internet Industry Association (IIA), etc. framed guideline provisions on both substantive and procedural law relating to cyber-crime. “However all these diversities in the legal responses towards a crime that has no natural boundaries and not amenable to national jurisdictions, only proves that the cyber crimes can’t be effectively dealt with by these individual efforts. What is needed is the global unification of the laws and procedures...........” * 104 The IT Act - however classified the various cyber wrongs into two groups. The first group described U/s. 43, deals with unauthorized access, image or injury to computer or network, denial of access, unauthorized downloading of data or information, injecting any injurious program like virus etc. These have been placed under civil management of adjudicating officer and cyber Appellate Tribunal.

And the other group of more serious offences like hacking (S/66) tampering with computer source code (S/65) publication or transmission of obscene material in digital media (S/67) have been placed under existing criminal law (S/80 power of police officer not below the rank of a DSP, S/78 power to investigate by DSP etc.) “Though, the focus of the Act is not on cyber crimes as such, the Act defines certain offences and penalties that deal with acts and omissions falling under the term cyber crimes. Chapter XI deals with penalties and adjudication. Chapter IX brings a welcome change in the minds of law makers as may be for the first time, Indian parliamentarians have come out of their obsession with the idea of ‘criminalisation’ as the sole means of regulating human conduct and upholding societal peace and tranquility and introduced civil liabilities as an alternative. Chapter IX reflects, the following features; Unique approach of regulating conduct; Premise is not to employ criminal but civil Regulation” * 105.

The Act however does not deal with Intellectual property issues in digital media but provides a basic framework for e-commerce transactions. The IT Act thus deals with recognition of electronic records (S/4 & S/14) digital signatures S/5 & S/15, electronic publication (S/8) rules of electronic communication (S/13) time and place of dispatch and receipt of electronic record. The Act however deals with security procedures in details and enacted (U/s. 87 & 16 of the Act) the Information Technology (Security Procedure) Rules - 2004 The G O I also prepared a broad based ISP Guide Line for setting up Internet Gateway and Service providers And the other instrument of the GOI is the Information Technology (Certifying Authorities ) Rules – 2000 for the better implementation of the IT Act provisions. “ 5th February 2002 , the memorable day in Indian E – commerce history, Controller of Certifying Authority , Government of India , has appointed first Certifying Authority, Safe Script , the joint venture of Verisign and Satyam Infoway Ltd.” *105A
3.4 ESSENTIAL FEATURES OF THE GOVERNANCE IN CYBER SPACE

For historical reason the US Government played a dominant role in Internet governance through A R P A and then through N S F. But on withdrawal of ARPA in 1990 and NSF in 1995 and on creation of private back bone lines, universal access, full scale commercial activities through the Internet etc. the US control i.e. unilateral authority has been diluted excepting"....Only as a means of protecting the stability of the organization and its' processes". 106 , Thus no centrally managed control mechanism operates in the Internet in technical aspect or in rule-making activities. The Communication lines simply carry the signals in the form of zeros and ones and the smart device at the end the computer, recovers the meaning there from. So it is observed by different authors that technical administrative functions of the Internet is a co-ordinate function participated by various non profit NGO like bodies. Due to the very nature of the Internet being borderless, no territorial and sovereign control is possible. It is observed that –

"Government controls in General as mentioned earlier, the Internet’s design precludes a central control, which may be regulated by governments. Nevertheless, governments are interested in what passes over their phone lines and are pursuing various means of exercising some degree of control by intercepting Internet communication" * 107

“Until recently, only Network Solutions Inc. (USI) carried out the registration and administration of the DNS for the COM, ORG and NET generic international top level names. Network Solutions Inc. is a private company which performs the function of registering Internet domain names ending in ‘Com’, ‘org’, ‘net’... ‘edu’, or ‘gov’. It registers over 1,00,000 new domain names each month, approximately one every 20 seconds. * (Academy of Motion Picture Arts and Science V Network solutions Inc: 989 F. supp. 1276-1277 (C.D. Cal. 1997). Today I C A N N has opened the domain name registration market to world wide competition employing one shared database, which is managed by NSI “ * 108, It is also observed that the Internet has always been governed. However it has always been regarded as more administrative co-ordination of a network by a few functionaries rather than as decision makers. The I A N A (Internet Assigned Numbers Authority) headed by the late John Postel, for instance, was ‘dedicated to preserving the central co-ordination functions of the global Internet for the public good. These functionaries, individual entities, were supported, funded or recognized by the US Government. In effect, key decisions with respect to the architecture of the Internet could only be taken by the US Federal Government....
Problems arising from the domain name system...as well as trademark domain conflicts-----finally provided......for the reformatory initiative. This initiative led to the incorporation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1999. a non-profit organization incorporated in California US. The legitimacy of this international, UN like entity to administer or govern to Internet has been ceaselessly questioned by various interest groups. The reason for this is simple and derives from the nature of the Internet itself.

"The Internet is not Government controlled, but neither is it controlled by commercial interests. It is global in nature, but there are no treaties or international agreements that govern it. The only inroad so far seems to be the efforts of WIPO to be recognized as a dispute resolution mechanism provider”. * 109 Again it is observed that ‘The Internet is a borderless phenomena and cyberspace does not fall within any national jurisdiction. There is already extensive literature on how individuals or Govt. anywhere in the world can easily launch an attack on US infrastructure or networks, and this attack can pass through several other countries in the process. This poses problems for assigning liability and for the enforcement of laws”. * 110, i.e. no central control does exist. It is also observed that “there are some forms of self governance in cyberspace that include engineers developing technological protocols, sysops and access providers creating and imposing terms and conditions of access on their users, as well as a set of rules, commonly referred to as ‘netiquette’ that mainly defines cyber manners. In addition, cyber space already possesses some enforcement mechanisms which include banishment from the server, shunning, mail bombs or cancel bots. The story of ICANN is an excellent example for effective self regulation in the cyber-space. Internet Corporation for Assigned Names and Numbers ((ICANN) is now looking after these services that were originally performed under US Government contract by the Internet Assigned Numbers Authority (IANA) and other entities ICANN now performs the IANA function.

ICANN is an internationally organized, non-profit corporation, that has responsibility for Internet Protocol (IP) address, space allocation, protocol identifier assignment, general (TLD) and country code (TLD) top-level domain name system management and root server system management functions.

.....Working collectively, ICANN,s participants address those issues that directly concern ICANN,s mission of technical co-ordination consistent with the principle of maximum self-regulation in the high tech economy, ICANN is

109 * Sup-32------------------------Edn. 2001 -------------------------------P - 5
110* Sup-73------------------Vol-II------Edn. 2005--------------------------P-20(3)
Perhaps the foremost example of collaboration by the various constituents of the Internet community (http://www.icann.org/), ICANN has proved that without direct regulation from the governments Internet can be as regulated or better regulated than any governmental structures. Here are various other voluntary initiatives in the Internet that strives to make it a better and safer place to be”. * 111

3.4(a) CRIME MANAGEMENT:

But this self-regulatory mechanism co-ordinated by ICANN & ISOC is not effective in crime management in cyber-space “However, the self-regulation in the cyberspace is not considered strong enough to deal with increasing criminality. The sanctions that are available to these self-regulating communities in the cyber space are not enough to deter potential criminal behavior. Therefore, it is in evitable that the state has to step in with some level of regulation of cyberspace”. * 112. Also that – “most of the self-regulation models base their sanctions on banishment from the group. Society may see such a sanction too light...So it is argued that some form of criminal sanctions is necessary to deter any destructive or antisocial conduct in the cyberspace this is not within the power of self-regulatory bodies and thus some interference form the states is inevitable *113, Thus crime management becomes an area of the general criminal jurisdiction of the sovereign. But so far the technical administrative functions are concerned, the centrally managed (actually co-ordinating bodies like ICANN & ISOC have been operative so long successfully.

But the growing political pressure as an instrument of corporate interest will sooner or later dominate the technical administration as well even at the cost of unrestricted global access. “By now everyone knows about the attempt by the US Commerce Department to’ recall’ the delegation of XXX to ICM Registry due to pressure from deluded rightwing groups in the US who think that it will add to pornography on the Internet. I want to argue here that this is a major inflection point in the history of ICANN and could represent the beginning of the end of its private sector/civil society based model of governance.

The issue is not merely an assertion of censorship powers over top level domains, but the sudden assertion of authority through the GAC to delay, overrule or veto decisions made by ICANN’S own processes and its Board, this shifts the balance of power in ICANN irrevocably back to governments, and encourages anyone seeking an important decision to spend most if not all, of their time with governments” *114 The core technical administrative functions of Internet have so long been managed by autonomous non-governmental bodies but these bodies are experiencing growing political pressure. This may thus lead to the loss of autonomy and freedom of these bodies.

111 * Sup-34------------------------2004---------------------P-30
112 * Sup-34------------------------2004---------------------P-10
113 * Sup-34------------------------2004---------------------P-32
114 * Dr. Milton Mueller (IGP) – http://www.icannwatch.org/----download on 03-09-05
An extensive world wide debate has been started on the United States intervention in ICANN domain name policy when the US Commerce Department issued a letter dated 15 August 2005 to the ICANN prohibiting the registration of some domain names related to pornography in cyber space (Ref. www.icannwatch.org) The Internet Governance Project (IGP) a consortium of academics along with many other autonomous civil society groups reacted sharply against this intervention by US Department of Commerce. “IGP issues statement—opposing political—-Intervention in the Internet’s core Technical Functions-August 25, 2005 concerned about the long term implications of the Commerce Department intervention in ICANNs policy making process, which was prompted by censorship advocates targeting the, xxx domain, the Internet Governance Project has issued a statement and a call for public support of its position...The statement charges that the NTIA intervention “undermines assurances from the US and from ICANN that it would never be used to shape policy but was only a means of protecting the stability of the organization and its processes”. UN – WIG also upheld the view of multi stakeholder approach to the Internet Governance.

The UN ICT Task Force observed in March 2004 “The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that (9) policy authority for Internet related public policy issues is the sovereign right of states... (b) The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields; (c) civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role, (d) Intergovernmental organizations have had and should continue to have a facilitating role in the co-ordination of Internet related public policy issues; (e) International organizations have also had and should continue to have an important role in the development of Internet related to technical standards and relevant policies.”

Thus distinct role of state, and private sector and civil society groups have been a practical reality in Internet governance at present.

115 * Internet Governance Project------------------Syracuse University-
http:// dcc.syr.edu/igp-home.htm----P-I----------download----08-09-05

116 * UN-ICT Task Force----http://www.unicttaskforce.org-para-49......download-08-09-05
The first Summit (WSIS) under UN-WGIG in Geneva was held in December (10-12) 2003.

The recent Tunis Summit (UN-WGIG) i.e. 2nd World Summit on Information Society (WSIS) is held on 16th November 2005. The independent role of ICANN has been found to be under pressure of US Commerce Department to monitor the registration of domain names. "The US government has won its battle to retain control of the Internet under a compromise worked out ahead of this week's UN Summit on the Information Society which leaves the current addressing and traffic direction system intact. "* 117 The Summit has decided to form an Intergovernmental Forum to manage some new problems based on cross border issues as web viruses, cyber crime and spam.

3.5 E-GOVERNANCE IN INDIA

Ref. – Ch-6.2.1 -------P-200