CHAPTER 7: MEASURES FOR COMBATING CYBER CRIMES

"Ultimately, there will be only one choice: It's not going to be feasible to extensively regulate the Internet because it'll be so easy to route around it." [1]

Brynjolfsson [2]

1. INTRODUCTION

In a world in which technology is developing at very fast rate and one cannot predict as to how it will impact on the coming generation. The Internet has completely changed the way we communicate. The catch phrase like 'global village' and 'information super highway' are no longer adequate enough to express the true dimensions of Internet explosion.

The Internet has often been characterized as an evolving network of networks, however, due to advance in technology, this description has become inadequate. With the growth of Internet, there is continuous growth of technology, which makes the use of Internet more straightforward. Internet access is no longer restricted to computer mainframe technology as it once was.

Recognizing the power of Internet to influence our social values, one of the most burning issues is the appropriate regulation of Internet. Many have criticized the mere suggestion of such regulation, citing violations of the US Constitutions First Amendment rights, or holding that such restrictions would challenge the original purpose of the Internet itself. Inspite of such arguments the debate continues. Much of the discussion centers upon the issues such as: Can we combat cyber crimes by regulating the Internet? What type of safeguards should be put in place in order to protect the rights of netizens? And lastly, who should be in charge?

2. INTERNET REGULATION – A LEGAL CHALLENGE

The Internet has given rise to number of legal questions. For example, if a copyrighted file is placed on the Internet, it can be copied easily without any degradation of the information. How should copyright be dealt with in the context of the Internet? If a defamatory statement is placed on a website, it is accessible to millions of users simultaneously. How can we track down the culprit, and where should we bring him to justice? In a space where physical boundaries do not mean anything, how shall we determine jurisdiction? If a hacker hacks into a computer system half way across the world, which legal system should we use to convict him? How would extradition work in such a situation? All these are very important questions.

Before we take initiatives to regulate Internet, it is necessary to understand what the Internet is and how it works. We have already discussed in detail as to what is Internet and how it works, so there is no need to go in detail again. We will just touch to one definition of Internet and proceed further.
What is the Internet? Benzine and Gerland gives us the following definition:
(a) Generally (not capitalized), any collection of distinct networks working together as one.
(b) Specifically (capitalized), the world wide "network of networks" that are connecting each other into one single logical network all sharing a common addressing scheme (using the IP protocol and other similar protocols). The Internet provides file transfer, remote login, electronic mail, and other services.

From this definition it can be inferred that the Internet is nothing more than thousands of networks that are connected to each other (usually by way of telephone lines). The mechanism that enables the computers of the world to understand each other is a set of uniform rules that lays down the basic foundation of understanding between different computers. This is known as the Internet Protocol.

The Internet provides five basic services, namely [3]

- electronic mail (e-mail);
- discussion lists (ListServs) and newsgroups (Usenet);
- File transfer protocol (FTP), and Telnet;
- Gopher
- World Wide Web (WWW).

Two of these services, namely electronic mail and the World Wide Web, dominate the whole Internet.

At the out set it is worth mentioning here, that while designing the Internet, the engineers took into account how a telephone network system might be disrupted when exposed to the attack of a nuclear bomb. As a result of this, the system was designed in such a way that if one or more of the components (known as "nodes") of the ARPANET would fall away, the remaining components will simply "route around"[4] the failing components. As time progressed, the network grew with leaps and bounds. The pure military purpose of the ARPANET gave way to a more general purpose of information sharing.

Thus, the Internet is simply a vast number of computer networks linked together by a single protocol that enables them to "speak the same language". This means that the different computer systems may run totally different software, but an "interpreter program" translates the information in such a way that the specific computer system may understand it [5].

Before discussing on the regulation, it is worth mentioning here that the massages passed through Internet are broken into small packets. This discussion in brief becomes important at this juncture becoze through this we will learn that Internet by itself was made decentralize. Thus, when the user presses the "send" button on his computer, the computer has to prepare the message for sending. This means that the computer will break up the message into so called "data packets" which is commonly known as data grams. After the message is broken up, the computer assigns a number to each individual data packet. The packets are then sent one after the other. When the different packets reach the router, the router decides where to send it next. Many

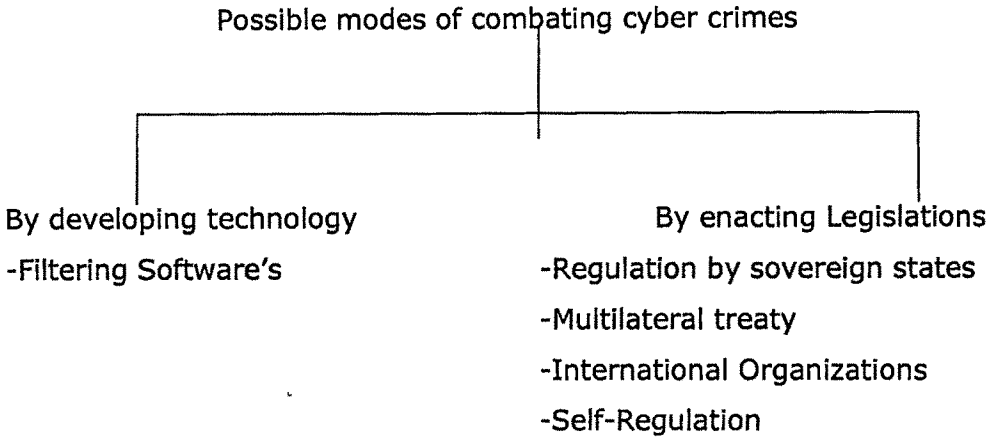
factors influence the router's decision, and as a result of this the different data packets will travel totally different routes to the destination. It is not uncommon for a single data packet to be routed hundreds of times. The data packet therefore "hops" [6] from the one router to the next until it reaches its destination. Because the datagrams travel totally different routes to the destination, it so happens that datagrams sent last may easily reach the destination before datagrams sent earlier on. This, however, poses no problem for the receiving computer. By using the same protocol, the receiving computer simply places the datagrams in its logical order, composes the message into a single message again (i.e. the way that the sender has sent it), and places the complete message into the receiver's e-mail box. The receiver can then retrieve the message whenever he wants to.

From a legal point of view it is important to understand how message is sent. By understanding how a message is broken up and sent via different routes, one can appreciate the problems that can occur when determining jurisdiction. It frequently happens that a single message will traverse the boundaries of many different countries, and if every country through which a datagram travel should attempt to exert jurisdiction, the process can become very complex and unmanageable.

The amazing feat of this whole process is that it takes place within a matter of seconds. The user does not even know that multiple requests have been sent between the browser, name server, and host. It is also interesting to note that each of these messages traveled a different route. In the process it might have traveled through routers in many different countries.

3. POSSIBLE WAYS TO COMBAT CYBERCRIMES

Combating cyber crimes becomes because of its decentralised nature. However, below mentioned could be some of the possible ways to curb cyber crimes.



When attempting to regulate the Internet, one can adopt following two (or either of two) methods:

A). The *first* possible mode through which we can curb cyber crimes is by using technological methods. This means we can develop certain software's/programmes that will prevent/filter out the unwanted material. However, this approach is disputed. It is found that it is not possible to develop any such full proof software.

B). *Another* mode, through which we may curb cybercrimes, is by enacting legislations. Here an attempt is made to regulate Internet by enacting suitable piece of legislations (e.g. Information Technology Act 2000) Thus it a regulation by creating the laws with different sanctions and principles. Under this approach if a person violates the law then he has to face sanctions by way of penalty.

Therefore, we can have two broad approaches i.e. legislation and/or physical regulation. We shall discuss first of all – a physical approach to regulate the Internet.

A). Regulation by developing technology

This approach covers various efforts on our part to regulate the content. It includes methods like installing filtering software's etc.

Filtering software

This approach takes into consideration, various technological methods like installing filtering software to regulate the content. Such filtering software provides two options:

Firstly, either the software blocks all sites that the user has indicated as being unacceptable and leaving other sites accessible. (This approach will most likely to be chosen by parents for themselves. This will enable them to surf the net without fear of stumbling onto unwanted sites.)
Secondly, allowing access only to some pre-determined sites and blocking the rest of sites. (Parents will most likely to follow this approach when they are allowing their children's to surf the net.)

Different filtering software's like Net Nanny; Cyber Patrol etc. can be used to filter out unwanted content. This filtering software provides different facilities. For example some filtering software uses the keywords to filter the content. For e.g. if filtering software used is programmed to filter out all sites containing the word 'sex', it will discard all such information where such word is found. The limitation of such software is that even if the site is educational, it will discard such site. Further such programme will not discard a pornographic picture file with a 'non-pornographic' name like 'misadro.gif'. Thus at this stage it is not possible for computer to recognise a pornographic picture file as such. Nextly, there are certain filtering software that lists certain IP (Internet Protocol) address, as being unwanted and if an attempt is made to access such site the computer will not permit it. However, this method has also some limitations. It would be next to impossible to list all the sites on the World Wide Web that are objectionable. Even if one would succeed in doing this, the site can easily be moved or mirrored to another location, which is not affected by the list. In such case the whole process of filtering will became meaningless.

Thus from the above discussion it can be inferred that filtering software cannot be the only solution to regulate the Internet. Although this method may prove to be very helpful in regulating the Internet, one must also look at other methods to resolve the problem.

B). Regulation of Internet through legislations

After discussing on the regulation of the Internet by using filtering software's, we now discuss as to how cyber crimes can be controlled by enacting legislations to that effect. Johnson and Post in their article, "And How Shall the Net be Governed?" lays down four possible methods for regulating the Internet. They are: -

Firstly, Sovereign states can enact laws that will be applicable in their respective jurisdictions. Thus, according to this first method, enacting legislations can curb cyber crimes.

Second possible mode to regulate Internet is to sign a multilateral treaty at global level. This multilateral treaty can then regulate the Internet extensively from a global perspective.

Thirdly, we can establish an International Organization to make new rules applicable to the Internet.

Fourth aspect deals with self-regulation. Johnson & Post says that, the Internet can be left to regulate itself. In such a model, governments should sit back and allow the Internet Service Providers and individual users to make rules that affect them [7]. These groups and persons will then, in effect, be the rulers of Cyberspace.

We shall now discuss each aspect separately.

FIRST - Regulation by a sovereign government

This is one of the most accepted for curbing cyber crimes. Under this approach every sovereign state will have freedom to regulate the Internet as it deems fit. This mode of regulation has been adopted by many states because there is, at present, nothing better to replace it.

Let us see at how different countries have attempted to regulate the Internet from within its boundaries.

United States Of America

At the outset it is wroth mentioning here that, The United States Of America is the most connected country in the world. This is, however, not surprising, as the Internet started in the US by way of the ARPANET project. More than 60 percent of all sites in the world are located within the United States [8].

It is also not surprising that the United States government was not so serious about regulation of Internet. This is a country where freedom of speech and expression has major significance. Therefore, the US government has not shown much interest in this field and has tried to maintain a low profile. However, seeing that the Internet is also dangerous if left totally unregulated, the US government has started to introduce new laws to address specific Internet related issues. The most notable of these are the attempts to regulate pornography and spam [9] on the Internet.

The very first attempt to regulate pornography on the Internet came by way of enacting the Communications Decency Act (CDA) [10]. This Act, which is a separate part of the new United States Telecommunications Act of 1996, had the purpose to regulate pornography on the Internet to such an extent that it would not be accessible to minors. This, of course, was a very worthy cause, but unfortunately the Act was drafted in a very poor fashion.

Two sections of the CDA is worth mentioning:

The first provision [11] prohibits "the knowing transmission of obscene or indecent messages to any recipient under 18 years of age"[12].

The second provision [13] prohibits "the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age"[14].

The American Civil Liberties Union (ACLU), an organisation that promotes freedom of speech in the US, challenged the constitutionality of the CDA. The three-judge district court held [15] that the CDA abridges the freedom of speech

principal as embodied in the First Amendment to the US Constitution. The decision was taken on appeal to the United States Supreme Court [16], which upheld the decision of the district court. The Supreme Court affirmed the decision of the district court because it said that the CDA went far beyond its purpose, even to such an extent that it infringed upon normal citizen's rights to freedom of speech. The court remarked that:

"The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in Ginsberg and Pacifica, the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all non-profit entities and individuals posing indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. ... It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library" [17].

After the termination of CDA, number of new bills has been drafted. The United States Congress is considering at least five bills [18]. Their topics range from forcing Internet Service Providers to provide filtering software [19], to prohibiting access to "sexually violent" offenders [20].

The term "spam" is a general term that is used to refer to unsolicited (junk) e-mail on the Internet. The spam battle illustrates when it might become necessary to regulate the Internet. One of the major Internet Service Provider in the US is America Online (AOL). Most of the new Internet users obtain America Online accounts, and they are the users that are most susceptible to spam. Because of heavy spamming, its servers have had to deal with major traffic congestions. To minimise this problem, AOL have introduced new software filters to filter out the spam. Spamming companies, which make a considerable amount of money by sending out spam on behalf of their customers, found a way to trick the spam-filtering software of AOL. This practise is known as "spoofing", and involves the creating of a false return address. Thus the spamming of AOL continued.

AOL filed suit against Over the Air Equipment, a spamming company, accusing it of using deceptive practices to bypass AOL's spamming filters. The Virginia district court ruled in favour of AOL, and Over the Air equipment had to pay AOL a "substantial but undisclosed" amount in damages [21]. Since this judgement has been given in October 1997, AOL has instituted similar proceedings against at least two other spamming companies [22].
In an attempt to curb the spammming problem, the US Congress is currently considering at least three new bills to regulate spam [23]. Hopefully these bills will be more properly worded than the CDA.

In July 1997, President Clinton and Vice President Gore announced a plan for making the Internet more "family friendly" [24]. After consultation with Internet Service Providers, the following agreement was reached:
- The online industry will report activities involving child pornography to law enforcement officials;
- Internet Service Providers undertake to remove all child pornography from their sites;

Gore announced that he would issue a parent's guide to the Internet; the National Center for Missing and Exploited Children would set up an emergency toll-free hotline where parents could report suspicious or illegal Internet content.

The clumsily titled- Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism Act of 2001 *(USA PATRIOT Act, or USAPA)* introduced a long legislative change, which significantly increased the surveillance, and investigative powers of law enforcement agencies in the United States. The Act did not, however, provide for the system of checks and balances that traditionally safeguards civil liberties in the face of such legislation. Legislative proposals in response to the terrorist attacks of September 11, 2001 were introduced less than a week after the attacks. President Bush signed the final bill, and it came into force on Oct. 26, 2001. The US PATRIOT Act retains provisions appreciably expanding government investigative authority, especially with respect to the Internet.

It seems as if the US is slowly realizing that an easygoing approach to regulate the Internet will not be enough. A more hands-on approach to regulating the Internet seems inevitable. However, the question whether it is feasible to legislate the Internet in a comprehensive manner, still remains unanswered.

INDIA

There is no general data protection law in India. In June 2000 the National Association of Software and Service Companies (NASSCOM) urged the government to pass a data protection law to ensure the privacy of information supplied over computer networks and to meet European data protection standards. The National Task Force on IT and Software Development had submitted an "IT Action Plan" to Prime Minister Vajpayee in July 1998 calling for the creation of a "National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data." It examined the United Kingdom Data Protection Act as a model and recommended several cyber laws including ones on privacy and encryption. No legislative measures, however, has been considered to date.

In May 2000, the government passed the Information Technology Act; a set of laws intended to provide a comprehensive regulatory environment for electronic commerce. The Act also addresses computer crime, hacking, damage to computer source code, breach of confidentiality and viewing of pornography. (The detail coverage of the Act has been done in Chap. 2).

Apart form Information Technology Act 2000, various other offences like Fraud, Cheating, Defamation via Internet will fall under various provision of Indian Penal Code 1860. Further certain amendments are also done in IPC and Evidence Act so as to keep pace with the developing technology.

Section 29A of the Indian Penal Code has been added by way of amendment. It lays down that the word "Electronic Record" shall have same meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act 2000. Also amendment in Indian Evidence Act 1872 has been made so as to accept electronic document by way of evidence. Section 47A,

deals with the opinions to digital signature, whereby the court may consider that signature if it is issued by certifying authority.

Following the enactment of the IT Act the Ministry of Information Technology adopted the Information Technology (Certifying Authorities) Rules in October 2000 to regulate the application of digital signatures and to provide guidelines for Certifying Authorities. The Digital Signature regime in India has become operational with effect from February 2002.

There is also a right of personal privacy in Indian law. Unlawful attacks on the honor and reputation of a person can invite an action in tort and/or criminal law. The Public Financial Institutions Act of 1993 codifies India's tradition of maintaining confidentiality in bank transactions. In March 2000 the Central Bureau of Investigation set up the Cyber Crime Investigation Cell (CCIC) to investigate offences under the IT Act and other high-tech crimes. The CCIC has jurisdiction over all of India and is a member of the Interpol Working Party on Information Technology Crime for South East Asia and Australia. Similar cells have been set up at the state and city level, for example in the state of Karnataka and the city of Mumbai. In June 2002 the central government authorized the National Police Academy in Hyderabad to prepare a handbook on procedures to handle digital evidence in the case of computer and Internet-related crimes. The government is also considering establishing an Electronic Research and Development Center of India to be responsible for developing new cyber-forensic tools. India's Intelligence Bureau is reported to have developed an e-mail interception tool similar to the Federal Bureau of Investigation's Carnivore system, which it claims to use in anti-terrorist investigations. In April 2002, India and the United States launched a cyber-security forum to collaborate on responding to cyber security threats.

The Corps of Detectives (COD), the specialized investigation agency of Karnataka, will soon set up the countries first cyber crime police station to tackle newer and innovative crimes using computers and the Internet. The COD Headquarters in Bangalore would be a "virtual station' with the jurisdiction covering the entire state to check such malpractices. In 1999 Karnataka

became the first state in country to set up a cyber crime investigation cell. Since then it had been concentrating on equipping the states police personnel with necessary resources to tackle cyber crimes. (See - www.Kannada.indiainfo.com)

Canada

The problem has not been as dramatically confronted in Canada, as it has had in the United States. While the Canadian approach will naturally differ from that of the United States, there is still much to be learned from the "American experience." The U.S. Supreme Court through a decision reviewing the case of ACLU v. Reno (June 1996) -- a judicial review of the Communication Decency Act -- confronted the issues raised by control of content on the Internet. This ground-breaking case, which has generated major judicial precedents in the U.S. concerning censorship on the Internet, will be of continuing interest to those making policy, legislation, and law with respect to the regulation of content in Canada and elsewhere.

In 1996, apparently in response to one of Information Highway Advisory Council (IHAC's) recommendations, the Government, through Industry Canada, commissioned an Internet Content-Related Liability Study. Four lawyers were appointed and directed to produce a report on the potential legal liabilities of ISP's in providing access to the Internet. Subsequent to the IHAC report and initiatives of the Clinton-Gore administration in the U.S., the Government of Canada has exhibited considerable interest in promoting international discussions concerning the control of content on the Internet. Most recently, Lloyd Axworthy, the Minister of Foreign Affairs -- citing the usual concerns about terrorism, drugs, obscenity and child pornography -- has stressed the need for a global policy on content.

Confronted with the failure of 'gate-keeping' by governments and the Courts or through direct legislation such as the Communication Decency Act in the U.S., politicians have now turned to a second method of control or regulation of Internet content through the use in the private and/or public sector of filtering/blocking software produced by commercial software or shareware designers, which permits parents, employers, Internet Service Providers or

public institutions to block the flow of specifically designated content. In Canada Information Highway Advisory Council (IHAC) obviously had already supported the need for a technology to filter or block offensive material.

Apart form the filtering software Part V of Canadian Criminal Code covers cyber crimes like Sexual offences, Public Morals and Disorderedly conduct. Section 151, 153 and 163 deals with various provisions relating to sexual offences. Further Section 163.1 of the Canadian Criminal Code defines specifically Child Pornography.

163.1 (1) In this section, "child pornography" means
(*a*) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,
(i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
(ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; or
(*b*) any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.
(2) Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of
(*a*) an indictable offence and liable to imprisonment for a term not exceeding ten years; or (*b*) an offence punishable on summary conviction.

Further sub cl. 3 and 4 of S.163.1 makes Distribution and Possession of Child Pornography a punishable offence. Even accessing to child pornography has been made criminal offence punishable with imprisonment for a term not exceeding five years. Even mailing of such obscene material is made punishable offence with imprisonment of two years. (s. 168).

The creation of IHAC broadly focused public, and particularly media, attention on the problem of controlling information on the Internet. Intensified by media coverage in Canada, there immediately followed a growing public concern with the purported dangers of the Internet with respect to permitting children to access information about: explosives; terrorism; drugs; all modes of sexual activity; indecent and offensive speech, including "hate speech"; permitting various predators, especially pedophiles opportunities to stalk children; and various pornographers, and rapists to threaten or harass women. Subsequently, there has been substantial debate regarding the extent of these purported dangers and the extent, if any, to which the specific introduction of the Internet has increased them.

Nevertheless, a global alarm about the Internet had been sparked off. It has been widely accepted in Canada that the Internet should be subject to those laws governing hate literature, child pornography and obscenity and that Internet Service Providers may well have some liability with respect to the materials they transmit. As well as being prosecuted for crimes, ISPs might be sued for defamation or for assisting in violations of copyright.

China

China believes it has the answer to Internet regulation: "eliminating what is undesirable and keeping what is good" [31]. China believes that the Internet is a tool to aid business and trade. Only these sectors are important as far as the Internet is concerned, and any other information is not given any special protection. It seems that China wants to attempt to block all information that is not related to business. They foresee having a Chinese portion of the Internet whereby all citizens within the country have free access to information within China, but when foreign content is to be accessed, permission is to be obtained from the government. At this stage free access to the Internet within the boundaries of China is reserved to a small number of carefully selected individuals, most of which fall within the science and computer industry [32]. Regulation of the Internet in China began in February 1996, when the government required Internet Service Providers to use only government-provided phone lines. Now users must also register with the police, and must

sign a pledge not to harm China's national interests. At present all traffic to and from China is routed through two major gateways in Beijing and Shanghai. Firewalls prevent access to specific Internet addresses, including many overseas newspapers and sites related to human rights and Taiwan and Tibetan politics. Some of these sites are blocked permanently, while others, like the sites on the anniversary of the 1989 Tiananmen Square protest, are only blocked during specific times [33]. The police in China actively patrols cyberspace by keeping track of Chinese surfers and their whereabouts on the Internet. This is, however, a enormous task, and users can only be tracked at random.

On the 11th December 1997 the Chinese State Counsel approved new regulations to further clamp down on the Internet in China. These regulations, consisting of twenty-five articles, came into force on the 30th Dec. 1997 [34]. Under the new regulations, Internet Service Providers would be subject to supervision by Public Security officials and would be obliged to help track down violators. Apart from this a number of new crimes were created that cover a wide range, including leaking state secrets, political subversion and spreading pornography and violence on the Internet. Internet Service Providers and users that break the law are subject to fines of up to 15 000 yuan ($ 1500.00).

Singapore

Regulation of Internet by Singapore is harsher than China. Internet Service Providers are controlled by the Singapore Broadcasting Authority and must abide by the strict guidelines regarding "objectionable content". This could range from pornography to "areas, which may undermine public morals, political stability or religious harmony" [35]. Furthermore, each Internet Service Provider must be registered with the government, and can be held liable for any content it gives access to.

However it is found that this is totally unacceptable. Holding an Internet Service Provider liable for content that it gives access to, is pointless, as the Internet Service Provider cannot know which sites all its users access. Many public access premises, for example schools, libraries, and cyber cafes, are required to install filtering software. Only "persons of standing" may operate

content relating to politics and religion, and such content must then be registered with the Singapore Broadcasting Authority [36].
The approach of legislating cautiously when looking at the Internet may prove to be the most sensible option at this early stage of the attempt to govern Cyberspace.

From the discussion above it can be inferred that many countries have made some or other attempt of regulating the Internet by way of legislation. A question that arise from this is, how effective can such laws be? As internet disregards the geographical boundaries, and sovereign laws are only applicable within the its jurisdiction, the question arises as to, what will the case if the wrongdoer is located in foreign country.

The case of Playboy Enterprises, Inc v Chuckleberry Publishing, Inc. illustrates the jurisdictional problem. In 1981, Playboy obtained an injunction against Chuckleberry Publishing, stating that Chuckleberry Publishing may not continue with their own "Playmen" publication, as it was very similar to the Playboy trademark. In January 1996, the defendant created an Internet website using its "Playmen" mark. The site was created and the server was located in Italy. Playboy filed suit in the United States, arguing that the defendant had violated the 1981 injunction by distributing the prohibited publication, albeit on the Internet. The defendant argued that he was "merely posting pictorial images on a computer server in Italy, rather than distributing those images to anyone within the United States. A computer operator wishing to view these images must, in effect, transport himself to Italy to view [the defendant's] pictorial displays. The use of the Internet is akin to boarding a plane, landing in Italy, and purchasing a copy of Playmen magazine, an activity permitted under Italian law" [37]. The court disagreed with this contention, and held that: "Defendant has actively solicited United States customers to its Internet site, and in doing so has distributed its product within the United States". The court further held that the defendant could operate his web site, but that he was prohibited from accepting any subscriptions from customers in the United States.
The interesting part of this case is the question of enforcement. If the defendant fails to comply with the order, how can it be enforced? Unfortunately

the court did not shed any light on this question. Why is jurisdiction such a problem when applying it to cyberspace? The answer to this lies within the realms of cyberspace itself.

Cyberspace is a place where the borders are totally different than in the "real world". However, it would be incorrect to say that cyberspace does not have any borders at all. Some servers and web sites require passwords to enter, and if one does not have the correct password, access would not be allowed. These sites are, however very few. Most of cyberspace is accessible to all Internet users, irrespective of where they may find themselves. The concept of jurisdiction as we currently know is very much related to geographical boundaries. While in case if Internet, it disregards the territorial limits. It is not unusual for a single web page to be composed of content that is obtained from different servers located in different countries in the world [38]. Some times the user has no way of knowing where the information originated.

Up till now we have discussed as to how sovereign states can put their efforts to tackle the problem of regulating the Internet. It is also found that attempting to regulate the Internet at a national level cannot work always due to the global nature of the Internet. An attempt can be made to regulate Internet at International level. We discuss some aspects relating to that.

SECOND - Multilateral treaties

The world is divided into number of sovereign states, which has its own geographical boundaries. Each sovereign state has the power to regulate his affairs within his state. But, it is also true that we live in a world where states are mutually dependent on each other. As a result of this, it has become necessary to regulate the relationships that countries have with each other. This falls within the area of International Law.

Another possible way through which Internet can be regulated is to sign a multilateral treaty. This might seem like the logical thing to do, but here again we also have to face certain objections. Internet has silently infiltrated our

lives, and before any active steps were taken for its regulation, it has become a part of our lives. In the early days of space exploration, jurists saw the whole space program on television and in the news, and knew that they were watching the creation of a new sphere of the law. International lawyers wrote about space exploration long before it took place [39], and when space travel became feasible, General Assembly resolutions and Space treaties [40] were already in place. This is, of course, totally different in case of Cyberspace. The latter surprised us because it was so close to us. The question that now arises is that, would it be possible to regulate the Internet by way of a multilateral treaty?

At the moment we do not have any treaty that attempts to regulate Internet. The only treaty that vaguely relates to the Internet is the Agreement on Basic Telecommunications Services [41], which is regulated under the auspices of the World Trade Organisation. According to this agreement a signatory state will guarantee to provide access to the basic telecommunications infrastructure, and undertakes to see to it that anti-competitive behaviour in the industry is curtailed. It seems, therefore, that this agreement can at most only apply to the Internet in so far as the providing of physical telephone lines go. South Africa is a signatory to the agreement. Would it be feasible to regulate the Internet by way of a treaty? Johnson and Post do not believe so. They feel that this will lead to more problems than solutions.

Firstly, the treaty process is very slow. Once treaty is signed it takes much time to enter into force. This poses a particular problem in cyberspace. As technology develops very fast, by the time treaty is enforced things may change totally.

Secondly, even if such treaty is drafted, it will most probably be a high level document written in very 'general' form. Johnson and Post says that, the problems usually present themselves in the details - especially in the context of the Internet. For example, a new technological problem may be encountered where a rapid resolution is needed to exploit the potential of the new technology. Treaty law will most probably not be able to meet this need.

It is submitted that both the criticisms that Johnson & Post raise against the Multilateral treaty-method, are totally correct. It is true that the treaty process is very slow, and it is equally true that Internet technology develops very fast.

THIRD - International Organisation

The third possible mode of Internet regulation that Johnson & Post looks at is the creation of an International Organization [42]. According to this mode an International Organisation could be created to "regulate the Internet". The organisation will have the power to make any decision that relates to the Internet, and make rules to compel enforcement.

The question is could this form of organisation work on such a global level? And again how could such a government impose its rules on the Net as a whole if all countries have not agreed to it? By what right should they be allowed to govern? The answer to this question lies in how the International Organization is created. If a single country (or a very small number of countries) attempts to establish an International Organisation, the International Organisation will not have any right to govern Cyberspace. The reason is a country cannot attempt to bring an International Organisation into being if it does not have the considerable consensus from the majority of countries of the rest of the world. However it is also true that such an organisation do exist. The American Registry of Internet Numbers (ARIN), which was formed in 1997 and started its work on 22 December 1997, is good example. This organisation is responsible for the allocation of IP-addresses, but instead of exerting its power only within the jurisdiction of the USA, it is also responsible for the allocation of IP-addresses in South America, the Caribbean and sub Saharan Africa [43]. This organisation was not created by any multilateral treaty, but simply by means of incorporation under the Virginia Nonstock Corporations Act [44]. Further more, ARIN has obtained its authorisation from the Internet Assigned Numbers Authority (IANA), which was commissioned by the US Defence Department to address the issuing of IP-numbers and was equally unrepresentative of the rest of the world. If one looks at the history from where the authority to issue IP-addresses came from (the US Defence Department), one can understand how

the allocation of IP-addresses was managed, especially when the Net was in its infancy. However, the Internet is now a truly global network, and an important function like assigning Internet numbers should be managed by an International Organisation that is truly representative.

It is found that the initial question of Johnson & Post as to "how could such an International Organisation be truly representative", is not fully correct. It is submitted that, the answer lies in the way that the organisation is formed. If the organisation is formed by way of agreement of many countries, it will have the necessary authority to regulate the Internet. Johnson & Post also have another objection, "What would keep such a governance mechanism from being captured by factions?" [45]. This is of course, a matter of serious thought. It is rightly said, 'absolute corrupts absolutely', and therefore if someone is having full control over the flow of information, he will literally have the "world at his feet". Information is a very powerful commodity, and a monopolisation thereof could be disastrous.

It is submitted that International Law has already found a solution to this problem. The answer lies in another area of the law, i.e. the International Civil Aviation Industry. In 1945 delegates were faced with a new challenge to regulate an industry that transcended borders, and that could only be truly regulated on a global scale. That industry is, of course, the Civil Aviation Industry, and the delegates faced with the "new global challenge", came up with a novel idea. They decided to create an International Organisation by way of a multilateral treaty. By doing so, they created an organisation that could operate with the blessing of many countries. The International Organisation is, of course, the International Civil Aviation Organisation, which is still functioning very well after more than fifty years of existence [46].

The delegates at the 1945 conference knew that if a single force is allowed to infiltrate the ICAO for its own benefit it will substantially affect the whole Civil Aviation Industry, which is worth billions of dollars each year. In order to prevent such an infiltration from taking place, they structured the ICAO in such a way that it is virtually impossible to monopolies it. This argument becomes

even clearer when we see exactly how the ICAO is structured. The ICAO is structured very much like the United Nations. It has a sovereign body, the Assembly, a governing body, the Counsel, and a Secretariat, which is tasked to execute the decisions of the former decision making bodies [47]. The assembly of the ICAO is composed of representatives from all contracting states (182 countries currently), and meets at least once every three years. This body's function is to make all the policy decisions affecting the Civil Aviation industry. The Counsel of the ICAO is a permanent body responsible to the Assembly and is composed of 33 contracting states elected by the Assembly for a three-year term. In the election, adequate representation is given to States of chief importance in air transport. Although the structure of the ICAO might seem elaborate, it is necessary to have it in such a fashion as to ensure the safety of the organisation. By introducing "checks and balances" in such a way, the democratic existence of the organisation is secured.

Johnson & Post believe that there is no room for an International Organisation in Internet regulation. It is submitted that if a truly representative International Organization (having considerable support for majority of countries) is created to deal with Internet related problems, it could help in governing Cyberspace.

FOURTH - Self-regulation of Internet

Another mode of Internet regulation that Johnson & Post proposes is "self-regulation-model". According to this mode the Internet should be allowed to govern itself. Netizens may group themselves into certain communities, whereby they will be having the same standards to be followed.

For example, instead of making rules that regulate spam, the user should be allowed to subscribe to an Internet Service Provider that allow their users to receive spam (if that user wants to receive spams). In the same way is a does not want to receive spam he can subscribe to an Internet Service Provider that does not allow spam on its system. Thus, under this mode the Internet Service Providers should be left alone to regulate themselves.

Johnson & Post believes that this system should be followed to regulate the Internet. According to them, it is the ultimate form of democracy. The self-regulation model relies heavily on a principle that the rules of Cyberspace should be made by the system operators (i.e. Internet Service Providers), but should be enforced by sovereign countries. Johnson & Post formulates it as follows: ".... the premise of the decentralised means of net governance is that the nations of the world would agree to enforce the rules established by Internet Service Providers and user interactions, just as they now enforce contracts entered into by private parties" [48].

Although it is true that sovereign countries enforce contracts that private parties enter into, it is something totally different from making the rules for Cyberspace. When two persons sign a contract, they make rules for themselves that fall within the boundaries of law of contract. In such a case the government may enforce such rules, because it falls within the jurisdiction of that government. But what if the parties to the contract transgress the principles of contract law. In such case, the government will not be ready to enforce the rules. For example, if Indian Contract Act states that a written agreement needs a signature from both parties, it will not enforce the contract if the signatures are omitted. The case of the system operator or user making the rules in Cyberspace is totally different. In such a case the system operator or user will make the rules, which may not fall within the contract law. In such case it is not possible for the sovereign states to enforce such rules.

Yet another objection is, if governments are not ready to enforce rules laid down by Internet Service Providers and users, who will enforce those rules? In the self-regulation model it is clear that the rule making process is done in a decentralised way. If a central government is not prepared to enforce those rules, the rule makers will similarly not be in the position to enforce them, because they are mere specks in the whole decentralised rule making Cyber world. In such a case the whole self-governing model of Internet regulation will fail. There is another point of criticism against this mode is it will not be adequate to determine complex legal issues such as copyrights, free speech, obscenity, or fraud.

The last doubt to the self-regulation model is, if Net is left to regulate itself, a numerous rules will exist simultaneously. This will confuse the people, as it would be difficult for them to know what are there rights and duties. Thus we have discussed four modes of Internet regulation that Johnson and Post discuss in their article, "And How Shall the Net be governed?". Each of these models has their advantages and drawbacks. It is submitted that each of these models could successfully work in certain circumstances. Instead of looking at these four models of Internet regulation as mutually exclusive, as Johnson and Post do, we should attempt to establish where each of these models could perhaps find its place.

4. PROPOSED METHOD FOR INTERNET REGULATION

> *The courts and the legislatures of the world will apply the law to the Internet. Rather than ask, "should the Internet be regulated?" it would be more germane to question, "what is socially desirable?" and "how can we best balance the conflicting interests of the users of the Internet?"* H Jarvlepp

(A). Applying all the possible modes to regulate net

As there is no one method to regulate Internet, grouping of different methods may prove to be helpful. In real world, subjects are governed by the rules that are framed by geographically based sovereign states. These rules and regulations will be applicable within the territorially based borders. But when we talk about Internet, things are totally different. In cyberspace there is no authority to regulate it, as it totally disregards the territorial boundaries. In case of Internet it is Internet Service Providers who may be called to be the actual entities who may regulate the Internet.

Thus, we have two kinds of worlds: *Firstly*, a 'real world', which is based on geographically based countries, and which is governed by governments, and, *Secondly*, a 'cyberspace', which consists of different networks (that are electronically divided from other networks) which are governed by Internet Service Providers.

Here there exists two different sets of rules and therefore it becomes difficult to regulate Internet. For example, jurisdiction in the 'real world' is established by physical geographical boundaries, but while we talk about 'cyberspace', the same geographical boundaries become totally irrelevant. The real problem is how to combine these two worlds. It becomes difficult, while we try to involve the government, to play a important part in regulating cyberspace. The question here arises is, why we want to combine the two worlds? Why don't we simply establish rules for cyberspace and let the Internet Service Providers regulate the cyber world? The reason is simple. Although the Internet Service Providers can regulate the cyberspace, they do not posses the power to make rules in the real world. They cannot make laws and enforce it in the real world. In that sense they are "swords without edges". To put it in another way - although cyberspace is different from the "real world" it exists within the real world. Cyberspace is changed to "real world". The citizens of cyberspace are also citizens of the "real world", although they are located in different countries. When we look at enforcement mechanisms, we will have to look at the "real world". The culprit lives in the real world, and it is only there that we can get to him.

Before discussing different ways to govern cyberspace, one another important concept needs to be discussed. It is true that in real world, it is the government that is who has the power to make rules for a particular territory. However, in case of cyberspace there is no single government to control it. The authority to govern the whole of cyberspace can only be exercised on a global scale, because only on a global scale does such an authority exist. If a country wants to govern cyberspace, it must accept that it cannot attempt to apply its rules to the whole of cyberspace. It can, at most, only bind its own Internet Service Providers, by framing rules and regulations within its territorially.

Before establishing rules for the governance of cyberspace, following premises must be understood:

- Cyberspace is a separate territory in the world;
- Cyberspace exists within the "real world";
- Internet Service Providers have the power to govern cyberspace, but not the "real world";
- Governance of the whole of cyberspace can only be done on a global scale;
- Territorial sovereigns cannot govern the whole of cyberspace, but at most the
- Internet Service Providers within its territorial boundaries.

(B). How can Cyberspace be governed?

(1) Multilateral treaty

As already discussed earlier, it is only on global level one can frame the rules that could regulate Internet. Therefore a multilateral treaty would seem to be the appropriate method to establish such ground rules. However, this method has certain limitations. A multilateral treaty might be appropriate to lay down the most fundamental rules of cyberspace. But, there may be difficulty in enforcing these rules. Cyberspace is changing very fast and treaty process may not be able to keep pace with the change. It may lag behind the rapid technological advances.

(2) International Organisation

Secondly, an International Organization may be created to deal with this issue. If we can create an International Organisation that is accepted by the majority of states in the world, it can make more detailed decisions that affect the Internet. Such an organisation can rapidly answer burning issues, and can enforce it because it has the authority of sovereign states. For example, we already have such a system in place, but in another sphere of the law. We are referring to the Civil Aviation Industry, and the International Organisation that successfully governs it for the last 52 years is called the International Civil Aviation Organisation.

Assuming that such an International Organisation can be created, the next question that arises is, how it should govern the cyberspace. The answer to this might be found by drawing an analogy to the "real world". In the "real world" we find, in general, two kinds of territories:
Firstly, we find territories that fall within the control of a sovereign state.
Secondly, we find territories that do not fall within the exclusive control of a sovereign state, but is at the disposal of all nations. Examples of the latter kind of territory would be the high seas, Antarctica and outer space. In the same way, the cyberspace may be divided into two categories: (1) General territory and (2) Special territory.

General territory may include all the majority of information that can be found on the Internet and which is appropriate for any person including children's. If an Internet Service Provider places any undesirable information on this territory of Internet, he can be held liable for doing so.
In case of *Special territory*, the Internet Service Providers may decide to provide access to those users only that meets specific requirements (which could be laid down by International Organization). Apart form this, the entrance to this special territory may be in such a way that, if any information is send from special territory, the network computer will add a special tag/or code to the content. These tag/code will then specify the user that he is accessing special territory. Parents may activate the filtering software to filter any information that is accompanied with this "special network" tag". From the above discussion it is clear that Internet Service Providers can play a vital role in regulating the Internet. It is therefore essential that the International Organisation should, if created, lay down rules governing Internet Service Providers around the globe. These rules should only establish the minimum standards that are required of an Internet Service Provider. An example of this would be to oblige the Internet Service Provider to place pornographic sites in the "special territory" of the Internet. (It is submitted that it will be the task of the International Organisation to lay down rules on what kind of information should be displayed on the "special territory" of the network).

Another question that arises is that, what if such an organisation is given the authority to regulate the Internet on a global scale, what would the role of individual countries be? The main problem here is, the different ideological differences between countries. The United States and China can be taken as an example. Whereas the United States believes in freedom of expression, China believes in the regulation of ideas and information. Finding a middle ground may prove to be ineffective, as it might alienate both countries to the idea of creating an International Organisation. The probable answer to this is, the International Organisation should only lay down minimum standards. The countries may be allowed to regulate by way of higher standards in their own territory. If, for example, any country wants to prohibit pornography altogether, it should at least be given the right to attempt to regulate it.

(C). Enforcement mechanisms

Even if we succeed to regulate the Internet, it would be useless if we cannot enforce the rules. Enforcement mechanisms are therefore of primary importance. Thus, if all the signatory states give the International Organisation the power to make rules, and also the power to enforce it across boundaries, it will be of great use. Secondly, we shall have to look at an "International Internet Adjudication System".

For example, Professor Perritt (Perrit "Jurisdiction in Cyberspace: the role of intermediaries" http://www.law.vill.edu/harvard/article/harv96k.htm (Expired Link) 08/01/1998) believes that an International Criminal Court might be the answer. The International Law Commission is looking at the possibility of establishing a permanent International Court. However, if one looks carefully at the function that the International Criminal Court is most likely to fulfill, it is clear that Internet crimes will not be included in the list of crimes destined for the court. Art 20 of the draft Statute of the Permanent Criminal Court (Report of the International Law Commission, 46th Session, UNGAOR, 49th Session, supp. No. 10 UN Doc. A/49/10 (1994) states that only the so-called "core crimes" will be brought before the International Criminal Court. These core crimes are crimes such as genocide, aggression, serious violations of the laws and customs applicable to armed conflict and crimes against humanity. Not even the most serious treaty crimes are listed in

the statute, because it will meet serious opposition from those countries, which did not sign the treaties that brought the specific crimes into existence. It therefore only refers to crimes, which are most probably jus cogens. Less serious Internet crimes will therefore not fall within the jurisdiction of the International Criminal Court.

(D). Critical Evaluation of Proposed Model

The methods that are discussed above suffer from some drawbacks.

(1) Multilateral Agreement

The first criticism against this method is that, a multilateral treaty is a very slow instrument to use, and in case of Internet the same problem may continue. Another, more practical problem is the fact that if we make the use of a multilateral treaty to establish ground rules for the Internet, it will be of primary importance that it receives support from The United States. The reason is, majority of websites in the world are launched from the USA, and if the treaty is not supported by the USA, its implementation will be very difficult. Thus, USA is in a superior position in respect of Internet regulation. Drafting a treaty to accommodate all the role players might be difficult.

(2) International Organisation

It is submitted, that an International Organisation might be established to deal with Internet related problems in a quick manner. However, the process of establishing such an organisation might take a long time, as it will most probably have to be done by way of a multilateral treaty. Many Internet related problems that needs urgent attention, might have surfaced in the meantime.
Again, if an International Organisation is formed, it might seem as if sovereign countries are merely handing over their power to the organisation. If perceived in such a way, many countries might be reluctant to give their consent to such an organisation being created. Lastly, there are also chances that such an organisation might be taken over by propagandists for their own vested gain.

(3) General & Specific Territory

Creation of general and specific territory may seem logical but it will be difficult to convince all the Internet Service Providers to comply with it. Again, if an Internet Service Provider is allowed to make the rules for his specific territory of the network, to what extent will he be allowed to make his own rules? This might prove to be a difficult question.

5. CONCLUSION

The uncontrollable Internet brings the global community together and closer. The Internet without national boundary does not belong to any single organization or country. The development of the Internet also goes beyond the control of any organization or country. Because of the unique nature of the Internet, the need for international cooperation to curb cyber crimes has come on the agenda for the global community. International cooperation will create an environment where international dialogue, remedies and solutions can be achieved between the global communities, and will educate and create awareness of the vulnerabilities to cybercrime for the ultimate protection against any financial, and intellectual property loss. International cooperation will surely provide a network of expertise from the global communities where talent and broad-based practical knowledge and skill is immediately accessible to all members of the community.

Cyber crimes, a new type of crimes, came with the Internet and will flourish with it unless the international community does not work together to control it. International community should strive for maximum cooperation between nations in order to address the potential for tremendous economic losses and the general threat to the safety, privacy and other fundamental values.

It is submitted that there cannot be not be one universal model for regulating the Internet. But this does not mean that we should stop our persistent efforts for regulating the Internet. It is hoped that the model might lead towards a greater understanding of the problem of Internet regulation, and could assist in the formulation of a solution to this very indefinable challenge.

Footnotes

1. What Brynjolfsson means is that the Internet consists of so many nodes, that if a particular node should become ineffective, the Internet will simply route the information to another router. This system was specifically designed to assure that the initial ARPANET should still function if a nuclear attack should damage a substantial part of the telephone network. Jarvlepp "An Introduction to the Law of the Internet" http://www.inforamp.net/~jarvlepp/kbsum95.html
2. Bowman "China Crackdown Could Thwart E-Commerce" http://www.zdnet.com/zdnn/content/zdnn/1231/267788.html
3. Benzine and Gerland "Accessing and Using the Internet" 1995 United Nations Statistical Division 82.
4. Ibid 3
5. Bowman "China Crackdown Could Thwart E-Commerce" http://www.zdnet.com/zdnn/content/zdnn/1231/267788.html
6. The term "hopping" from the one router to the next is a very common jargon phrase among computer experts.
7. Johnson & Post "And how shall the Net be governed?" 9/5/96 http://www.cli.org/emdraft.html
8. Reno, Attorney General of the United States, et al. v American Civil Liberties Union et al http://www.aclu.org/court/renovacludec.html
9. "Spam" is an Internet term, which refers to unsolicited e-mail (junk e-mail).
10. Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).
11. 47 U.S.C.A. §223(a).
12. Ibid (n 33).
13. 47 U.S.C.A. §223(d).
14. Ibid (n 33).
15. American Civil Liberties Union v Reno, 929 Esupp. 824 (E,D. Pa. 1996).
16. Reno, Attorney General of the United States, et al. v American Civil Liberties Union et al http://www.aclu.org/court/renovacludec.html
17. Reno, Attorney General of the United States, et al. v American Civil Liberties Union et al http://www.aclu.org/court/renovacludec.html
18. (a) Selling Online pornography to minors; (b) Net access and sexual predators; (c) Protecting Children from Internet Predators Act; (d) Family Friendly Internet Access Act; (e) Internet freedom and Child Protection Act. Macavinta "Online speech: Porn, spam, and political disclosure" News.com http://www.news.com/SpecialFeatures/0,5,16873,00.html
19. Family Friendly Internet Access Act and the Internet freedom and Child Protection Act. Macavinta "Online speech: Porn, spam, and political disclosure" News.com http://www.news.com/SpecialFeatures/0,5,16873,00.html
20. Net access and sexual predators. Macavinta "Online speech: Porn, spam, and political disclosure" News.com http://www.news.com/SpecialFeatures/0,5,16873,00.html
21. Kornblum "Antispam efforts heat up" 14 November 1997 News.com http://www.news.com/News/Item/0,4,16393,00.html

22.The two companies are Squeaky Clean Marketing and Cyber Services. Pelline "AOL Wins Latest Spam Battle" 18 December 1997 http://www.news.com/News/Item/0,4,17490.00.html
23.The three bills are: The Netizens Protection Act, the Unsolicited Commercial Electronic Mail Choice Act, and the Electronic Mailbox Protection Act. Macavinta "Online speech: Porn, spam, and political disclosure" News.com http://www.news.com/SpecialFeatures/0,5,16873,00.html
24."Family Friendly Internet" http://www.whitehouse.gov/WH/New/Ratings/
25.Nash "Holding Compuserve Responsible" 15 January 1996 New York Times.
26.Although the German Constitution guarantees the right to free speech, some forms of expression, including certain types of pornography, are explicitly excluded.
27.Meyer "A Bad Dream Comes True in Cyberspace: The Germans Cencor an Online Service and the Rest of Us Too" Newsweek 8 Jan 1996 65.

28.Delacourt "The International Impact of Internet Regulation" 1997 Harvard International Law Journal 213.
29.A mirror site is a site that looks exactly like the original site (it is a "mirror" of the original site), but which is located at another server in another county, province, or country than the original site. The mirror site, however, has a different IP-address than the original site, and as a result of this it might be possible to access the mirror site whilst access to the original site is denied.
30.IuKDG art 1(5), par 1.
31.Khan et al "Chinese firewall: Beijing Seeks to Build Version of the Internet that Can Be Censored: Crackdown of Outside Views also Includes Satelite TV and Financial News Wires" Wall Street Journal 31 Jan 1996.
32.Mufson "China Opens a Window on Cyberspace: Growing Use of Internet Spreads Information, Once Banned Ideas" Washington Post 19 June 1995.
33."Countries face cyber-control in their own ways" The Los Angeles Times, Posted by CNN http://cnn.com/TECH/9707/01/cda.countries.lat/index.html (Expired Link) 05/01/1998 at 12.42.
34."China clamps new controls on Internet" Reuters, Posted by CNN at http://cnn.com/WORLD/9712/30/china.internet.reut/index.html
35."Countries face cyber-control in their own ways" The Los Angeles Times, Posted by CNN http://cnn.com/TECH/9707/01/cda.countries.lat/index.html (Expired Link) 05/01/1998 at 12.42.
36."Countries face cyber-control in their own ways" The Los Angeles Times, Posted by CNN http://cnn.com/TECH/9707/01/cda.countries.lat/index.html (Expired Link) 05/01/1998 at 12.42.
37.Donohue "Litigation in Cyberspace: Jurisdiction and Choice of Law a United States Perspective" 1997

http://www.abanet.org/buslaw/cyber/jiusjuris.html (Expired Link) 17/12/1997 16:41.

38. An example of this would be where web site A produces its own text, but graphics are imported from web site B, located at another server in another country. The actual graphic that will be displayed on web site A (together with the text), is never saved on the server of web site A. It merely tells the user's browser where to collect the graphic file.
39. Jenks "International Law and Activities in space" International and Comparative Law Quarterly (Vol 5) 99.
40. For example the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies 610 United Nations Treaty Series 205 and The Convention on Registration of Objects Launched into Outer Space 1975 17 International Legal Materials 43, to mention but a few.
41. "ISPA Submission to SATRA" 10 June 1997 http://www.ispa.org.za/submission2.html
42. Johnson & Post "And how shall the Net be governed?" 9/5/96 http://www.cli.org/emdraft.html
43. "Arin Initiates Operations" http://www.arin.net/opening.html (Expired Link)]
44. "Bylaws of American Registry for Internet Numbers" http://www.arin.net/docs/bylaw.htm (Expired Link)
45. Johnson & Post "And how shall the Net be governed?" 9/5/96 http://www.cli.org/emdraft.html
46. "Facts About ICAO" http://www.cam.org/~icao/facts.htm (Expired Link) 23/06/1997
47. Ibid 46
48. Johnson & Post "And how shall the Net be governed?" 9/5/96 http://www.cli.org/emdraft.html