Volume : 1 | Issue : 10 | October 2012 ISSN - 2250-1991

Research Paper Law

Regualting The Omnipresence Menace of Cyber Crimes

* Dr Solanki

* Associate Professor Faculty of Law The M S University of Baroda Vadodara

ABSTRACT

Stating that the Internet is a medium of unlimited possibilities is an empty declaration. Currently, no one can even fathom where the technological progress will take us in the times to come. Regardless of this, a few trends in the Internet are highly questionable. Its multimedia potential makes it a distinct medium to gather and exchange information; it breaks down all kinds of barriers-physical and mental, and it has a claim to being more prying and personal than any other technology. It is revolutionizing the business scenario and yet it is highly unorganized. In short, it is metamorphosing our way of life and we are not adequately aware of the ways. The paper aims to discuss various possible modes of regulating the uncontrolled Internet.

Keywords : Regulating the Internet, Uncontrollable Net, Internet regulation

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' is 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. It can be seen now that with the growth of Internet, there is also a continuous growth of technology, which makes the use of Internet more straightforward and easy. Thus, Internet access is no longer restricted to computer mainframe technology as it was once. The way Internet is regularizing our lives, it becomes evident that we need to answer one of the most burning issues and that is how to regulate Internet. There are critics also who says that regulating the internet would challenge the original purpose of the Internet itself. In spite of such arguments the debate continues.

INTERNET REGULATION – A LEGAL CHALLENGE

The Internet has given rise to number of legal questions. Questions such as regulating online fraud, defamation, gambling, jurisdictional issue, cyber pornography etc are some of the issues to which many government are not able to answer. The question arises is that in a space where physical boundaries do not mean anything, how to regulate Internet. 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. Nations around the world are very concerned about cybercrime, a concern shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe.[2]

Many legal challenges faced by police and prosecutors in pursuit of cybercriminals can be illustrated by the brief yet destructive career of the “Love Bug” virus.[3] The virus destroyed files and stole passwords.[4] Law enforcement officials cannot take action against cybercriminals unless countries first enact laws which criminalize the activities in which these offenders engage. As the “Love Bug” investigators learned, the existence of such laws is a fundamental prerequisite for investigation as well as for prosecution. It would therefore seem obvious that all nations would have or at least desire to have cybercrime laws on the books.[5] Before we take initiatives to regulate Internet, it is necessary to understand what the Internet is and how it works. The Internet is nothing more than thousands of networks that are connected to each other. The mechanism that enables the computers of the world to understand each other is a set of homogeneous rules that lays down the basic foundation of understanding between different computers. This is known as the Internet Protocol. At the outset 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”) would fall away, the remaining components will simply route around the failing components[6]. With the passage of time the network grew with leaps and bounds. The new mode of communication that was initially started for pure military purpose of the ARPANET gave way to a more general purpose of information sharing on commercial basis.

POSSIBLE WAYS TO COMBAT CYBERCRIMES

We now discuss the possible methods to regulate cyber crimes. This can be done by evolving a mechanism that shall regulate the internet at global level. Below mentioned could be some of the possible ways to curb cyber crimes.

a. Filtering software

Installing the filtering software is perhaps the most suitable m ethods to cut down the objectionable/unwanted content. This approach takes into consideration, various technological methods like installing filtering software such as Net Nanny; Cyber Patrol etc. These would help to filter out unwanted content. Unfortunately one of the limitations of this software is that even if the site is educational, it will discard such site. Thus filtering software cannot be the only solution to regulate the Internet.

b. Regulation by Sovereign States

Second possible mode which perhaps could work well at local level is that Sovereign states can enact laws that will be applicable in their respective jurisdictions. Thus, according to this method, enacting legislations can curb cyber crimes (For example The Information Technology Act 2000). To prevent the recurrence of another “Love Bug” scenario, the Philippines quickly adopted legislation outlawing certain types of cybercrimes, including the creation and dissemination of viruses. [7]

c. Multilateral Treaty

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

d. International Organizations

We can also think of establishing an International Organization to make new rules applicable to the Internet, and which shall apply globally.

e. Self Regulation

Lastly, we can try to regulate internet through self-regulation. Here the vital role should be played the Internet Service providers and individual users to make rules that affect them[8]. These groups and persons will then, in effect, be the rulers of Cyberspace.

PROPOSED METHOD FOR INTERNET REGULATION

Since there is no one method that can regulate Internet, it is advisable that grouping of different methods may prove to be helpful. As it happens in the real world, people are governed by the rules that are framed by geographically based sovereign states. Such rules and regulations will then 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. Here we see two kind of worlds: firstly, it is a 'real world' which is totally based upon on geographically boundaries, and the same is governed by the sovereign states, second world is of 'cyberspace', which consists of different networks, for which we don't have appropriate mechanisms for its regulations.

The problem that occurs is that how to combine these two worlds. 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 catch hold of them.

The difficulty lies in properly defining the laws needed to allow for cybercriminals' apprehension and prosecution. While seemingly a straightforward task, difficult issues are raised. One is whether the definitiona l scope of cybercrimes should include only laws that prohibit activities targeting computers or should outlaw crimes against individuals affected through the computer as well, such as cyber stalking and cyber terrorism. Another is whether these laws should be cybercrime-specific, targeting only crimes committed by exploiting computer technology.[9]

HOW CAN CYBERSPACE BE GOVERNED?

(1) Multilateral treaty

As already discussed earlier, signing a multilateral treaty is only a proper answer as of now. Unfortunately, this method has certain limitations. A multilateral treaty might be appropriate to lay down some of the most fundamental rules of cyberspace. But, the real problem lies 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 Organization

Secondly, if we can create an International Organization that is accepted by the majority of countries of the world, it may prove to be more effective solution. Such an organization can rapidly answer burning issues at global level, and can enforce it because it has the authority of sovereign states. Again, such International Organization may 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.

One question that arises here is that, what if such an organization is given the authority to regulate the Internet on a global scale, what would the role of individual countries be? The main problem in such case would be the different ideologies between different countries. The probable answer to this is, the International Organization should only lay down minimum standards. The countries may be allowed to regulate by way of higher standards in their own territory.

(C) Enforcement mechanisms

Even if we succeed to lay down effective regulatory measures for Internet, it would be useless if we cannot enforce the rules. Good enforcement mechanisms very important. If all the signatory states give the International Organization the power to make rules, and also the power to enforce it across boundaries, it will be of great use.

CRITICAL EVALUATION OF PROPOSED REGULATION MODES

The methods that are discussed above have certain limitations.

(1) Multilateral Agreement

The first criticism against this method is that, a multilateral treaty is a very slow instrument and thus 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 all the nations states, which may be a difficult task, as no sovereign state would like to surrender its sovereignty.

(2) International Organization

It is submitted, that an International Organization might be established to deal with Internet related problems in a quick manner. However, the process of establishing such an organization might take a long time, as it will most probably have to be done by way of a multilateral treaty. Again, if an International Organization is formed, it might seem as if sovereign countries are merely handing over their power to the organization. If apparent that many countries might be unwilling to give their consent to such an organization being created.

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. 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. It is submitted that there cannot be one universal model for regulating the Internet. But this does not mean that we should stop our persistent efforts for regulating the Internet.

REFERENCES

Dr. G A Solanki, Associate Professor, Faculty of Law, The M S University of Baroda | Cyber Crime and Punishment? Archaic Laws Threaten Global Information, MCCONNELL INTERNATIONAL (December 2000), at | http://www.mcconnellinternational.com/services/cybercrime.html , accessed on 8/9/12 | Technically, the "Love Bug" was both a virus and a worm: | Fiendishly created, the Love Bug strikes with a one-two punch. Once you've clicked open that fatal attachment and activated its deadly code, the virus either erases or moves a wide range of data files. It singles out in particular so-called .jpgs and MP3s — digital pictures and music — and, like a natural virus, replaces them with identical copies of itself. Then, if it finds the Microsoft Outlook Express e-mail program on your computer, it raids the program's address book and sends copies of itself to everyone on that list. . . . Technically, this two-pronged approach makes the Love Bug both a virus and a worm; it's a virus because it breeds on a host computer's hard drive and a worm because it also reproduces over a network. Lev Grossman, Attack of the Love Bug, TIME EUROPE, (May 15, 2000), available at http://www.time.com/time/europe/magazine/2000/0515/cover.html. For more on computer viruses and worms, see, e.g., Jeffrey O. Kephart, et al., Fighting Computer Viruses, SCIENTIFIC AMERICAN, accessed on 7/912, available at http://www.sciam.com/1197issue/1197kephart.html; Bob Page, A Report on the Internet Worm, accessed on 7/9/12, at ftp://coast.cs.purdue.edu/pub/doc/morris_worm/worm.paper; Computer Abuse: Worms, Viruses, Trojan Horses, at http://www.eos.ncsu.edu/eos/info/computer_ethics/abuse/wvt/. | See, e.g., Students Named in Love Bug Probe, APBNEWS.COM, available at http://www.apbnews.com/newscenter/internetcrime/2000/05/10/lovebug0510_01.html; accessed on 9/9/12, Rick Thomas, Love Bug Virus Is No Herbie, THE BUSINESS JOURNAL, available at http://www.thepbj.com/051200/a19.htm. , accessed on 10/9/12 | The Emerging consensus on Criminal Conduct in Cyberspace, by Mark Goodman and Susan Breener, available at http://law.scu.edu/international/File/goodmanbrenner.pdf, accessed on 10/10/12 | Benzine and Gerland "Accessing and Using the Internet" 1995 United Nations Statistical Division 82 | See, e.g., "Love bug" Prompts New Philippine Law, USA Today available at http://www.usatoday.com/life/cyber/tech/cti095.htm (under the new law, hackers and those who spread computer viruses can be fined a minimum of $2,350 and a maximum "commensurate" with the damage caused, and can be imprisoned for up to three years) accessed on 9/10/12. See also Republic of the Philippines, Eleventh Congress – Second Regular Session, Republic Act No. 8792, Part V § 33, available at http://www.mcconnellinternational.com/services/country/philippines.pdf. , accessed on 9/10/12 | | Johnson & Post "And how shall the Net be Governed?", available at http://www.cli.org/emdraft.html, accessed on 6/9/12 | | Ibid 4 |