THE REGULATION OF CYBERSPACE*

Charmaine H. Perdon[**]
Paul Dennis A. Quintero[**]

Technology ... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.

— C. P. Snow

The latter part of the twentieth century will be remembered as the era when information and communications technologies transformed the relationships between individuals, governments, and social institutions. Cyberspace, a computer-generated public domain which goes beyond traditional conceptions of time and space, is instrumental in diminishing the powers of the nation-state to govern its constituents. This is due to the increasing lack of control over both local and global communications in cyberspace. States have been increasingly concerned with passing legislation aimed at controlling the excesses committed in cyberspace, especially in the area of illegal activities committed through the Internet. However, for many people, cyberspace is a medium where empowerment and freedom from state control should always be maintained.[1]

However, there has been an increasing trend of state intervention in this previously uncontested domain. Issues of privacy, surveillance, and control are becoming the prime concerns brought about by state interest, along with crime control, security, and economic advantage. In the United States and Europe, legislatures have passed laws seeking to regulate the use of the Internet. Some of these laws are now in effect, though at least one United States law,

---

* 1999 Roberto Sabido Best Legal Paper Award

** Fourth Year LL.B., University of the Philippines College of Law.

[1] John Barlow, in his *Declaration of the Independence of Cyberspace*, said that it is from ethics, enlightened self-interest, and the common well that governance of cyberspace will emerge. See John P. Barlow, *A Declaration of the Independence of Cyberspace*, 56 THE HUMANIST 18 (1996).

the *Communications Decency Act*, was struck down by their courts as offensive to the United States Constitution.[2]

On the other hand, in other countries, especially those where the use of the Internet is just emerging, what governs is essentially a regime of self-regulation by the Internet service providers and users with minimum or no government regulation. The threshold problem is whether the State should intervene or regulate the Internet or allow the private sector to regulate itself. In case State regulation is chosen, what kind of laws should be passed by the State and how should these laws be enforced, without infringing on the constitutional rights of the private citizen?

The objective of this paper is not to enumerate each and every problem in the field of Internet regulation. This paper will instead attempt to provide a ***processual and holistic view*** of the realities and issues concerning the governance of cyberspace in the Philippines: the dilemma of whether or not to legislate controls over this domain; the adequacy or inadequacy of current laws as applied to cyberspace, the constitutionality of State intervention; and implementation and enforcement of regulation by the State.

I. CYBERSPACE AND ITS STRUCTURE

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation ... A graphical representation of data abstracted from the bank of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding....
>
> — William Gibson, *Neuromancer*[3]

Cyberspace is a new form of human interaction brought about by developments in information and communications technology. It is a computer-generated domain which has no territorial boundaries or physical attributes, and is manifested by the matrix of computer networks called the

---

[2] *See* Reno v. ACLU, 117 S.Ct. 2329 (1997).

[3] WILLIAM GIBSON, NEUROMANCER. The term "cyberspace" was first coined in this futuristic novel, wherein the characters accessed computers by merging their thoughts with a database.

Internet, linking people from all parts of the globe.[4] Cyberspace is usually depicted as a virtual common space, a collection of different multimedia technologies and networks which are held together by a standard computing protocol.[5]

While some information resources of the Internet[6] are relatively private (like electronic mail,[7] invited Internet chat,[8] or videoteleconferencing), others are more public in orientation, such as mailing list services[9] and

---

[4] Cyberspace is a unique medium having no territorial boundaries and available to anyone, anywhere in the world, with access to the Internet. This medium is a composite of the various tools or methods used to transmit text, sound, pictures, and moving video images, namely: electronic mail, automatic mailing list services (listserv), newsgroups, chat rooms, and the World Wide Web.

[5] The foundation of the World Wide Web is the millions of web pages created with a special language called the HyperText Markup Language (HTML). It was specifically designed to provide a standard for creating, sending, and displaying information in the form of pages on the Internet. HyperText Transfer Protocol (HTTP) is the standard communication protocol for sending and receiving HTML documents over the Web. The Universal Resource Locator (URL) identifies both HTML and HTTP when accessing web pages. It is a standard that allows you to enter the name and location of information, as well as the method for transporting that information over the Internet.

[6] The Internet is a network is a collection of computers connected to each other to achieve some common objective. Networks permit users to share information. It is a series of networks linked using very precise rules that allow any user to connect to and use any available network or computer connected to the Internet. *See* Reno v. ACLU, 117 S.Ct. 2329 (1997). The Internet is also a communication system that uses physical connections (usually telephone lines, direct wires, fiber optics, satellite transmissions, etc.) to link one computer network to another. The Internet has a standard of communication called a *protocol*, that enables one computer network to speak to another.

[7] E[lectronic] mail is one of the oldest and most popular uses of the Internet. *See* Comment, *Privacy and Encryption in Cyberspace*, 34 SAN DIEGO L. REV. 1401, 1402 n.2 (1997). Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. Messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic service provider. If the intended addressee subscribes to the service, the message is stored by the company's computer system until the subscriber calls the company to retrieve the mail. This is then sent over the telephone system to the recipient's computer. Electronic mail systems may be available for public use or may be proprietary, such as those set up and operated by private companies for internal communication. *See* Reno v. ACLU, 117 S.Ct. 2329 (1997).

[8] While one can post a message that can be read later by another, two or more individuals wishing to communicate more immediately or on a more or less real-time basis can enter a chat room and engage in a dialogue by typing messages to one another that appear almost immediately on the other person's computer screen. *See* Reno v. ACLU, 117 S.Ct. 2329 (1997).

[9] An automatic mailing list service is a form of electronic mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the other subscribers of the group. *See* Reno v. ACLU, 117 S.Ct. 2329 (1997).

web pages, the latter being found on the so-called "World Wide Web" (hereinafter, the Web).[10]

The structure of the Internet can best be explained by this analogy offered by one commentator:

> Envision a roadmap. Cities dot the otherwise sparse landscape and roads branch out in all directions, connecting every city. Although not every city is connected to every other, it is possible to reach any one city from any other. Like every other mass transit system, certain areas are more traveled than others. Some cities are larger than others and some stretches of road are more prone to traffic. The size and complexity of this roadmap defies the imagination — it encircles the world. But the cities are not actually cities. They are computers or groups of computers. The roads are telephone lines or fiber-optic cable. The system surrounds the globe in an electronic web of data. The travelers on these 'virtual' roads are packets of information which are sent from one city to another, perhaps via many. The roadmap is a worldwide computer "network." Each city is a depot or terminal for the packets, and is usually referred to as a "node." In reality they are mainframes owned by universities, companies, or groups of computer users.[11]

The Internet was a originally a creation of the United States military and defense departments. During the Cold War years, more specifically between 1957 and 1960, the U.S. Defense Department was preoccupied with preventing the prospect of a breakdown in communications facilities in the event of war or enemy attack.[12] The Defense Department assigned the problem to its Advanced Research Projects Agency (ARPA). The RAND Corporation proposed a solution: what is now called *Distributed Adaptive Message Block Switching* or *Packet Switching*. A message is cut into small pieces,

---

[10] The Web is the most popular category of communication over the Internet. It allows users to search for and retrieve information stored in remote computers, and in some cases, to communicate back to designated sites. *See* Reno v. ACLU, 117 S.Ct. 2329 n. 9 (1997). The Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. More complicated documents, called web "pages" are more widespread. Each web page its own address and functions like a telephone number.

[11] *See* Michael S. Borella, *Computer Privacy vs. First and Fourth Amendment Rights* (visited 8 January 1999) <http://www.eff.org/pub/Legal/comp_privacy_vs_rights.paper>.

[12] Peter H. Salus, *The Net: A Brief History of its Origins*, 38 JURIMETRICS J. 671 (1998). Key communications installations were often bombed by members of the "American Republican Army."

each of which is separately addressed. The objective of the network is to ensure that there are always available routes for the packets of information. Prior to the advent of packet switching, the communication structure was so problematic that when the wire between two machines was cut, communication was prevented. Packet switching works this way: If there are three machines and each one is connected to the other two, even if one wire is cut the other machines can still be accessed through the other branch.[13]

The Defense Department provided funds for several research arms of universities in the United States. Together with these schools, they set up the very first network through the use of the *Interface Message Protector* (IMP) which was connected to a "dedicated" phone line and on the other to the various host computers which string together mini-computers in the participating schools. The IMPs were thus the first routers, equipped to pass information from one place to another. The network soon grew and expanded to foreign countries. At present, practically every country in the world is connected or wired to the Internet.

II. STATE INTERVENTION OR SELF-REGULATION

A. Current practices in state regulation

1. Laws and other state actions specifically directed at regulating cyberspace

Because of the rapid growth in the number of Internet users, some governments have decided to put an end to the laissez faire regime under which the Internet community initially fell, requiring government authorization before new users are wired to the Internet, which is seen as a threat to state security. Others welcome the advent of this new medium but are concerned about its perceived negative effects.

Society's dependence on the computer has made it vulnerable to criminal activity carried out in cyberspace. All sorts of crimes are now being committed within the shadowy corners of the Internet. Threats to personal

[13] *Id.* at 672.

safety, property, and national security are magnified by the power of the Internet. The Internet can be used in all stages of criminal activity from planning the crime, marshaling of resources up to the point of execution.[14]

Some Internet advocates believe that the government should keep a hands off policy. However, many policymakers and those responsible for running the State believe otherwise. It seems inevitable that at least in the short term, the State will play an active part in the regulation of the Internet. Many countries around the world have already undertaken steps to combat abuses in cyberspace.

a. In the United States

i. The Electronic Communication Privacy Act (ECPA) of 1986

The Electronic Communication Privacy Act (hereinafter, ECPA),[15] enacted on October 1, 1986, amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968 — the Federal Wiretap Law — to protect against the unauthorized interception of electronic communications.[16] The ECPA attempts to strike a balance between the privacy expectations of American

---

[14] The following are just some of the instances of criminal activity perpetuated on the Internet.

a) The intellectual property rights of publishers are violated over the Internet.

b) Identity theft, whereby personal information is drawn from Internet databases and used for credit card applications by the thief, is now a cause of concern in many countries.

c) So-called cyberpirates register phantom ships on the computers of maritime agencies. They take huge insurance contracts and then they sink these non-existent ships and file million dollar insurance claims.

d) The Internet has now been used for electronic money laundering.

e) Animal poachers in Africa now take orders via electronic mail.

Other areas of concern include: (1) the posting of hard-core pornographic images, which can be accessed easily worldwide; (2) the posting of guidelines on how to make home-made explosives, a fact which came to the public's attention after the U.S. Senate hearings on the Oklahoma City bombing; (3) the use of the Internet by political extremists, racists and terrorists to propagate their doctrines and access each other's ideas and resources.

[15] U.S. Electronic Communications Privacy Act, Pub. L. No. 99-508 (1986) [hereinafter ECPA].

[16] In 1984, a U.S. Senator made a query to the Justice Department on the latter's opinion as to whether or not interceptions of electronic mail and computer-to-computer communications were covered by the Federal Wiretap Law. It was said in reply that there was protection only where a reasonable expectation of privacy existed. The Department opined that in the rapidly developing area of communications, whether or not there existed a reasonable expectation of privacy was not always clear or obvious. See S. REP. NO. 99-541, at 132 (1986).

citizens and the legitimate needs of law enforcement agencies. It expanded the coverage of the anti-wiretapping laws to deal with new and revolutionary forms of electronic communication and new methods and devices for surveillance,[17] because of the inability of the wiretap law to keep pace with the development of communications and computer technology.

Interception of real-time communications

Title I of the ECPA deals with the interception of real-time electronic, wire, and oral communications. The provisions of this title were crafted because of the extensive use of computers in the transmission, processing, and storage of information. Two of the major developments in Internet-related activities are remote computing[18] and electronic mail services. These services as well as providers of electronic mail make electronic copies of the private correspondence for later reference. These data are normally stored by the service provider for a period of time to ensure system integrity. The proprietary or privacy interest in that information of the entity who made that communication should not change. However, since the data are now subject to the control of a third party computer operator, the information may be subject to no constitutional privacy protection. There is therefore an avenue for the possible wrongful use and public disclosure by law enforcement authorities and unauthorized private parties. Before the ECPA, the laws provided little authority for the service providers to resist unauthorized access.

Any service provider who discloses the existence of an interception or surveillance will be liable for civil damages, except when the disclosure was pursuant to any of the exceptions in the law.

As explained by the U.S. Senate Judiciary Committee, it is not unlawful for the employees of providers of electronic communication services

---

[17] *Id.*

[18] Remote computing or Telnet allows the user to use any host computer on the Internet as if the user is directly connected. For instance, a user can connect to a certain university's computer system by having a valid password and permission to use that computer. When the user "telnets" to another computer, his computer operates as if the user were sitting in the school's computer laboratory. Another example would be professionals or businesses transmitting their records to remote computers to obtain sophisticated data processing services.

to intercept, disclose, or use customer communications in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the provider. The provider or electronic communication service may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These are monitoring functions, which may be necessary to the provision of an electronic communications service.[19]

A service provider shall not *intentionally* divulge the contents of any communication (other than one to such person or entity, or an agent thereof) *while in transmission* (real-time messages) on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.[20] Under the ECPA, the term "*intentional*" has a more limited meaning than its ordinary dictionary definition. It would not be enough that one voluntarily engaged in conduct or caused a result, but such conduct must have been the *person's conscious objective* or the result of his desire to engage in the conduct (or cause the result). It means that it is "*done on purpose.*" It is not meant to connote the existence of motive. The liability for intentional prohibited conduct is not dependent on the motive of the person that led the person to disregard the law. This emphasizes that *inadvertent* interceptions by the provider are not crimes under the ECPA.[21]

There are exceptions to the criminal prohibition on disclosure by the provider of the contents of real-time messages. First, the law provides that providers can make the disclosure (a) with the lawful consent of the originator or any addressee or intended recipient; (b) to any person employed or authorized, or whose facilities are used to forward such communication to its destination (i.e. communication intermediaries); (c) where such messages were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement

---

[19] S. REP. NO. 99-541, *supra* note 16.

[20] *See* ECPA, Pub. L. No. 99-508, § 201, (1986) (codified as amended at 18 U.S.C. § 2702(a)(1)).

[21] *Id.*

agency.[22] This provision will not apply if the provider monitors on purpose the conversations to ascertain whether criminal activity has occurred or is being undertaken.

If the system operator happens to violate a user's privacy rights under the ECPA, by such acts as posting private e-mail publicly for all to see, the ECPA gives the user the *right to sue the system operator.*[23] The system operator must then remove the public posting and can be held responsible for any money damages incurred due to the privacy violation. The ECPA also allows for recovery of attorney fees.[24]

The complaint must allege that an electronic communications service provider (or one of is employees) did any or a combination of the following:

a) disclosed the existence of a wiretap
b) acted without a facially valid court order or certification
c) acted beyond the scope of a court order or certification
d) acted in bad faith[25]

Relief to the aggrieved party may be in the form of (1) preliminary and other equitable or declaratory relief as may be appropriate; (2) damages; (3) attorney's fees and other reasonable litigation costs.[26]

The ECPA provides for a *good faith defense* for those who follow court orders or warrants or legislative or statutory authorizations, or a request from an investigative or law enforcement officer concerning emergency situations. *Good faith* includes the receipt of a court order that is valid on its face. The fact that the provider received said order entitles him to a dismissal of the civil action provided he shows that he acted within the scope of that order.[27]

---

[22] *See* ECPA, Pub. L. No. 99-508, § 102, (1986) (codified as amended at 18 U.S.C. § 2511(3)(b)).

[23] *See* ECPA, Pub. L. No. 99-508, § 201, (1986) (codified as amended at 18 U.S.C. § 2707(a)).

[24] The civil action must be commenced within two years from the date the claimant first had a reasonable opportunity to discover the violation. *See* ECPA, Pub. L. No. 99-508, § 201, (1986) (codified as amended at 18 U.S.C. § 2707(e)).

[25] Bad faith includes failing to read the order or collusion.

[26] *See* ECPA, Pub. L. No. 99-508, § 201, (1986) (codified as amended at 18 U.S.C. § 2707 (b)).

[27] *See* ECPA, Pub. L. No. 99-508, § 103, (1986) (codified as amended at 18 U.S.C. § 2520(c)(2)(d)).

Criminal penalties

The ECPA criminalizes the following acts relating to *interception of real-time messages:*

1) Intentional disclosure by a service provider of the contents of any communication (other than one to such person or entity, or an agent thereof) *while in transmission* on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipients.[28]
2) *Warning* any person that a law enforcement agency or officer has been authorized or has sought authorization to intercept electronic communication.[29]

The defendant must have knowledge that the law enforcement officer has been given an interception order.[30] His action must be undertaken with specific intent to obstruct, impede, or prevent the interception. An attempt to engage in the offense is also punishable.

An injunctive relief, distinct from the above criminal penalties, in favor of the government, may also be availed of by the State whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a violation of the ECPA. The court may enter at any time before final determination the restraining order to prevent a continuing and substantial injury to the State or to any person or class of persons for whose protection the action is brought.[31]

---

[28] *See* ECPA, Pub. L. No. 99-508, § 102, (1986) (codified as amended at 18 U.S.C. § 2511(3)(a)).

[29] *See* ECPA, Pub. L. No. 99-508, § 109, (1986) (codified as amended at 18 U.S.C. § 2232(c)).

[30] Under the ECPA, if government authorities desire to intercept or review messages on their own initiative, they must obtain the appropriate warrant from a judge or magistrate. In terms of seizing information, a government agent must obtain a warrant if he wants to read a message that is stored for less than 180 days on an on-line system. If a desired message has been stored for over 180 days, the agent only has to obtain an administrative subpoena from the proper government agency rather than go to court for an order. *See* ECPA, Pub. L. No. 99-508, § 201(a), (1986) (codified as amended at 18 U.S.C. § 2703 (a)).

[31] *See* ECPA, Pub. L. No. 99-508, § 110, (1986) (codified as amended at 18 U.S.C. § 2521).

User privacy agreements

With the introduction of the ECPA, privacy protection, *in the absence of a* user privacy arrangement between the Internet service provider and the user, now covers all forms of digital communications, including transmissions of text and digitized images, in addition to voice communication which was already protected under the old wiretap law.[32] The law also proscribes unauthorized eavesdropping by the government, all persons and businesses. It prohibits unauthorized access of stored messages in a computer system, and also unauthorized interception of messages in transmission.

Most of the provisions of the ECPA on the protection of the privacy interests of the user can be superseded by privacy agreements between the provider and the user. ***But when there is no user privacy agreement*** between operator and user the ECPA allows the operator to (a) configure the system to store all messages that pass through it; (b) access and review or read all stored messages that pass through the system. These *stored messages* include those in the addressee's mailbox waiting to be picked up by the addressee, and records of private discussions between users. The operator can review and read all the messages stored in its system but it cannot disclose these to anyone, except the government. If a message is accidentally obtained, and the system operator feels illegal activity is taking place over the system, the system operator is permitted to disclose the accidentally obtained information to legal authorities. The authorities then have the right to review these messages as much as they deem necessary to confirm the system operator's apprehensions.[33] *Since there*

---

[32] It is possible that a particular transaction may consist of both electronic communications and wire or oral communications. For instance, the transmission of data over the telephone is an *electronic communication*. If the parties use the line to talk to each other during the data transmission, then that aspect is a *wire communication*. A person overhearing one end of the telephone conversation by listening to the oral utterances of one of the parties, falls under *oral communications*.

As a general rule, a communication is an *electronic communication* protected by the Federal Wiretap Law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences.

[33] See<http://www.people_virginia.edu/~kln6q/infopaper.ECPA.html> (visited 23 January 1999).

is no user privacy agreement, the user has no cause of action against the operator for disclosing the stored message to the government.[34]

When there exists a user privacy agreement between provider/operator and user, the following are provided for by the Act: (a) as for stored messages in the operator's system, it can be agreed upon that the operator can disclose user messages to anyone he chooses; (b) as for live or real-time messages, it can be stipulated that the operator may intercept them.[35]

The provider/operator and the user can agree as to the level of privacy that governs them. In the United States, there are three levels of privacy protection currently being implemented, which are as follows:

a) Operators can run a strongly private system — the operator can prohibit himself from viewing messages in storage even though the ECPA allows for such viewing. (They cannot prevent government authorities from obtaining private messages with proper legal orders.)
b) Operators can maintain strong privacy but maintain the right to view private messages if need be.
c) Operators can run a system without any privacy given to the users.

As for real-time transmission of voice messages through the Internet, the ECPA is silent. This can be attributed to the fact that at the time of the enactment of the ECPA in 1986, there was no technology yet to provide a feasible telephone service on the Internet. It was only in 1996 that the two major browser makers, Netscape and Microsoft introduced versions of their respective browsers enabling a computer to be used like a phone.[36] That

[34] The ECPA does not prevent employers from looking through employee e-mail if they so desire. Employers have every right to view certain messages received by their employees, for whatever motive such employer may have. After all, the employee is given a privilege when he or she is given access to the on-line system. Appropriate behavior and proper judgment though should be exercised. In 1993, legislation was proposed in Congress entitled the Privacy for Consumers and Workers Act. The bill, which would have limited personnel monitoring in companies, failed to pass Congress.

[35] <http://www.people_virginia.edu/`kln6q/infopaper.ECPA.html>, *supra* note 33.

[36] Steven Levy, *Calling All Computers*, NEWSWEEK 43 (13 May 1996).

interception of said voice messages throughout the so-called Internet phone can be covered by the old federal wiretapping law because the computer terminal effectively serves as a telephone terminal.

ii. Communications Decency Act of 1996

Though the Telecommunications Act of 1996 dealt very little with the Internet, it should be considered as an important piece of legislation concerning the governance of cyberspace, because of Title V of the law, known as the Communications Decency Act of 1996 (hereinafter, CDA). It contains the two anti-pornography provisions which became the subject of the landmark case *Reno v. American Civil Liberties Union*.[37] These provisions are what are now known as the *"indecent transmission provision"* and the *"patently offensive display provision."*

The former provision, under section 223(a), prohibited the intentional transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in part:

> (a) Whoever —
> (1) in interstate or foreign communications —
> (B)by means of a telecommunications device knowingly —
> (i) makes, creates, or solicits, and
> (ii) initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under eighteen years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
> (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years or both.

[37] Reno v. ACLU, 117 S.Ct. 2329 (1997).

The latter provision, section 223 paragraph (d), prohibits knowingly sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides :

> (d) Whoever —
>
> (1) in interstate or foreign communications knowingly —
> (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
>
> (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years or both. (emphasis supplied)

There are two affirmative defenses to the above acts provided for in section 223 paragraph (e)(5). The first exempts those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. The second covers those who restrict access to covered material by requiring certain designated forms of age proof.[38]

In full, section 223 paragraph (e)(5) provides:

> (5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a) (2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) of this section that a person —

[38] Reno v. ACLU, 117 S.Ct. 2329 (1997).

> (A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or
>
> (B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

The law effectively requires that the provider initiate measures to block out children from viewing the offending materials. The government sought to force each provider to run its own user identification system, though providers were absolved of liability for material which did not originate from them, and for which they are not otherwise responsible.

The U.S. Supreme Court, in the *Reno* case, affirmed the decision of the District Court of Pennsylvania and struck down as unconstitutional both the "*indecent transmission*" and the "*patently offensive display*" provisions. It held that the provisions abridged the freedom of speech protected by the First Amendment.[39]

The Court ruled that the precedents cited by the government, namely *Ginsberg v. New York*,[40] *FCC v. Pacifica Foundation*,[41] and *Renton v. Playtime Theaters, Inc.*,[42] even raise doubts as to the constitutionality of the law.

The Court ruled that the doctrine in *Ginsberg v. New York* was not in point. The law involved in that particular case was one prohibiting the sale of material to minors which were deemed obscene for them, even if these were not considered obscene for adults. It was held that the law in *Ginsberg* was narrower than the CDA, in the following respects:

---

[39] U.S. CONST., amend. I: Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof or abridging the freedom of speech, or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

[40] 390 U.S. 629 (1968).

[41] 438 U.S. 726 (1978).

[42] 475 US 41 (1985).

(a) The *Ginsberg* law did not prevent parents from buying such material for their children, while the CDA did not allow for parental consent or parental participation in communication.
(b) The *Ginsberg* statute applied only to commercial transactions, while the CDA covered both commercial and non-commercial communications.
(c) The *Ginsberg* law clarified its definition of material that is harmful to minors by requiring that it must be "utterly without redeeming social importance for minors." The CDA had no definition of the term "indecent" and did not allow "patently offensive" material that has serious literary, artistic, political, or scientific worth.
(d) The *Ginsberg* law covered only persons under seventeen years of age, while the CDA included an additional year of those nearest majority.[43]

The court also differentiated the CDA from the regulation involved in *FCC v. Pacifica Foundation.*[44] In this case, the U.S. Supreme Court ruled for the validity of a ruling of the Federal Communications Commission that the afternoon broadcast of a recorded monologue entitled "Filthy Words" could have been the subject of administrative sanctions. The CDA, unlike the regulation in *Pacifica,* is "not limited to particular times and is not dependent on any evaluation by an agency similar with the unique characteristics of the Internet." The FCC order did not contain any criminal penalty, while the CDA did. The FCC order pertained to radio which historically has been extended the least First Amendment protection. The court noted that the Internet has no comparable history and that the risk of accessing indecent material on the Internet by accident is remote as compared to radio and television broadcasts which the court characterized as "invasive" media.[45]

It found many ambiguities regarding the scope of the CDA which rendered it susceptible to attack under the First Amendment. The words "indecent" and "patently offensive" would create uncertainty among speakers with regard to how the two standards relate to each other and their meaning.

---

[43] Federal Ban on Internet Indecency Struck Down on First Amendment Grounds, 66 US LAW WEEK 1015 (1997).

[44] 438 U.S. 726 (1978).

[45] Reno v. ACLU, 117 S.Ct. 2329 (1997).

The vagueness of such a content-based regulation and its criminalization of the acts provided in the law would create a chilling effect on the freedom of expression. The law was not carefully tailored for First Amendment purposes, a defect which the Court had deemed fatal to a content-based statute. Although the government has a valid interest in protecting children from potentially harmful materials, the CDA seeks to achieve this by suppressing speech that adults have a constitutional right to send and receive under American law.

b. In Asia

The People's Republic of China has opened its doors to the Internet without sacrificing its control over information. The Chinese government requires Internet users to course electronic communications through a series of *government sponsored filters* under the control of the Ministry of Post and Telecommunication and other state agencies.[46] Domestic Internet users are also required to *register* with the police. Service providers and users are "forbidden to produce, retrieve, duplicate, or spread information that may hinder public order." China, with the help of foreign companies like IBM and Sun Microsystems, has embarked on the creation of a national network that is linked to the outside world but capable of being censored and controlled by the State.[47] Singapore now requires all Internet providers to *register* with the national broadcasting authority with strict regulations on what practices are prohibited.

In Japan, the police arrested a man for posting and distributing nude images on his personal web page. Thailand is considering ways to stop the export of electronic pornography and the spread of anti-Thai sentiments through the Internet. Saudi Arabia, Bahrain, and Iran now have state-run filtering systems to screen pornography as well as religious and politically seditious materials.[48]

---

[46] Michael Meyer, *Whose Internet is It?* NEWSWEEK 59 (22 April 1996).

[47] *Id.*

[48] *Id.* at 60.

c. In Europe

Among the European states, the German government has been the most active in terms of Internet intervention. In December 1995, a Bavarian prosecutor protested to the giant service provider CompuServe that there existed more than 200 newsgroups containing sexual material that was considered in violation of German law. At that time, CompuServe lacked the technology to block the sites to its more than 100,000 German subscribers. What it did was to cut off everyone from the sites complained of, including its American subscribers. Now, Germany only prevents access to only five of the sites it originally objected to. In January 1996, Deutsche Telekom blocked the website of the neo-Nazi Ernst Zuendel, a Canadian resident whose postings were carried by a Californian service provider. His postings contained materials denying the Holocaust which violated another German law. The Californian provider refused to close the site saying that it was constitutionally protected free speech. The Germans blocked not just Zuendel's site but also the 1,500 sites or more sites of the American service provider.[49] CompuServe now has the technology to keep objectionable material out of Germany while making it accessible in other parts of the world.

In April 1997, German prosecutors indicted the local head of CompuServe for allegedly aiding in the dissemination of pornography and extremist propaganda on the Internet. A few days later, the government introduced pioneering legislation to regulate the Internet called the ***Information and Communications Services Bill.*** The law aims to fight illegal misuse of the global computer network. It aims to set standards for child protection in cyberspace. It defines which activities require regulation and which can be operated without any formal license or regulatory oversight.[50]

d. Development of sectoral codes of practice

There is a move to pursue the creation of sectoral codes of practice to specifically tailor user protection in the Internet to the systems and practices of industries or of parts of the public sector like health care, policing and welfare

---

[49] *Id.*

[50] *German Offers Bill to Police Internet*, PHILIPPINE DAILY INQUIRER, 23 April 1997, at B12.

services.[51] Codes aid in specifying ground rules for permissible activity in particular contexts. Sectoral codes of practice have been established in the data-protection industries of Netherlands, the United Kingdom, and other countries.

2. Present state of Philippine statutes affecting the Internet

Most criminal and commercial statutes in the Philippines were enacted before the Internet became a fixture in the public awareness. Thus, the coverage of these laws contemplates the traditional kinds of media existing at the time of their promulgation. These laws are often incapable of being interpreted as covering the Internet medium. Thus, it is important to survey the significant provisions of Philippine law which relate to the peculiar and specific issues now confronting the Internet. These issues, to which Internet users are exposed to, are the following:

a. Criminal activities

i. Obscenity and immoral doctrines

Article 201 of the Revised Penal Code, which covers immoral doctrines, obscene publications and exhibitions and indecent shows,[52] is

---

[51] BRIAN D. LOADER, THE GOVERNANCE OF CYBERSPACE 168 (1997).

[52] Article 201. Immoral doctrines, obscene publications and exhibitions, and indecent shows.

The penalty of prision mayor or a fine ranging from 6,000 to 12,000 pesos, or both such imprisonment or fine, shall be imposed upon:

(1) Those who shall publicly expound or proclaim doctrines openly contrary to public morals;

(2) (a) the authors of obscene literature, published with their knowledge in any form; the editors publishing such literature; and the owners/operators of the establishment selling the same;

(b) Those who, in theaters, fairs, cinematographs or any other place,

(1) exhibit, indecent or immoral plays, scenes, acts or shows, whether live or in film, which are prescribed by virtue hereof, shall include those which (1) glorify criminals or (2) condone crimes;

(2) serve no other purpose but to satisfy the market for violence, lust or pornography;

(3) offend any race or religion;

(4) tend to abet traffic in and use of prohibited drugs; and

comprehensive enough to cover many illegal activities committed through the Internet such as obscenity, promotion of violence or mayhem, and racism. It even appears that the phrase "*published ... in any form,*" in paragraph (2)(a) could be interpreted to cover even postings on the Internet. Even owners of websites containing the above undesirable materials, whether published in text or in a live action format, could be covered by the term "*those who, in theaters ... or any other place, exhibit indecent or immoral plays, scenes, acts or shows, whether live or in film*" if cyberspace will be considered for purposes of this provision as a "place." However, Congress, which passed this law in 1930, is not likely to have foreseen the emergence of the new medium of cyberspace when they passed the Revised Penal Code. There could be a liberal interpretation of the provision justifying the subsumation of acts done on the Internet within the intendment of the law but such liberal interpretation would be highly dubitable. Besides, there is the well-settled rule that penal statutes are to be strictly construed against the State and liberally in favor of the accused. Thus, amending the provision to clarify that the same acts committed through the new medium of the Internet is essential.[53]

---

(5) are contrary to law, public order, morals, and good customs, established policies, lawful orders, decrees and edicts;

(3) Those who shall sell, give away or exhibit films, prints, engravings, sculpture or literature which are offensive to morals. (As amended by Pres. Dec. Nos. 960 and 969.)

[53] The authors propose the following amendment to article 201 of the Revised Penal Code. The text in boldface signify the revisions proposed by the authors.

Article 201. Immoral doctrines, obscene publications and exhibitions, and indecent shows.

The penalty of prision mayor or a fine ranging from six thousand to twelve thousand pesos, or both such imprisonment or fine, shall be imposed upon:

(1) Those who shall publicly expound or proclaim doctrines through any medium, including those electronic in nature, openly contrary to public morals;

(2)(a) the authors of obscene literature, comment, proposal, image, or other communication, published, transmitted, or sent with their knowledge in any form or in any medium including those electronic in nature; the owners/operators of the establishment selling the same; the editors publishing such literature, comment, proposal, image, or other communication; or the owner of an interactive computer service who has the capacity to remove the offending material, but neglects to do so for an unreasonable period of time after being informed or having knowledge of the obscene material;

(b) Those who, in theaters, fairs, cinematographs or any other place or medium including those electronic in nature, exhibit, indecent or immoral plays, scenes, images, texts, acts or shows, whether live, in film, or in electronic form, which are prescribed by virtue hereof, shall include those which

(1) glorify criminals or condone crimes;

(2) serve no other purpose but to satisfy the market for violence, lust or pornography;

(3) offend any race or religion;

ii. Libel

The Revised Penal Code speaks of libel in the following manner:

> **Article 353. Definition of libel.** — A libel is a public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead.
>
> **Article 354. Requirement for publicity.** — Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown.
>
> x x x
>
> **Article 355. Libel, means by writings or similar means.** — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, shall be punished by prision correccional in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.

Criminal libel should be punished, regardless of the medium through which it is committed. However, a person charged with posting defamatory remarks on the Internet can argue that the legislature which enacted the provision could not have contemplated that on-line libel is within the meaning of "*writing ... or any similar means.*"

The person accused of making such defamatory remarks may even claim that someone used his name in posting such message or that someone enabled an unauthorized person to gain access to his website, and posted the message without his knowledge and consent. It is virtually impossible to

---

(4) tend to abet traffic in and use of prohibited drugs; and

(5) are contrary to law, public order, morals, and good customs, established policies, lawful orders, decrees and edicts;

(3) Those who shall sell, give away or exhibit images, films, prints, engravings, sculpture or literature or display or transmit through any medium including those electronic in nature such materials which are offensive to morals.

verify if indeed he is lying or not. A minor amendment of the provisions is necessary for the purpose of clarifying the laws on libel as it may apply on-line. New issues in pinning liability for libel on the Internet may arise because of the very nature of Internet message transmission.[54]

iii. Infringement of intellectual property rights

The Intellectual Property Code provides:

> Sec. 171.7. "Published Works" means works, which, with the consent of the authors, are made available to the public by wire or wireless means in such a way that members of the public may access these works from a place and time individually chosen by them (emphasis supplied) x x x
>
> Sec. 172. Literary and Artistic Works.
> 172.1. Literary and artistic works, hereinafter referred to as "works" are original intellectual creations in the literary and artistic domain protected from the moment of their creation x x x
>
> Sec. 173. Derivative works.
> 173.1. The following derivative works shall also be protected by copyright:
>
> x x x
>
> b) Collections of literary, scholarly, or artistic works and compilations of data and other materials which are original by reason of the selection or coordination or arrangement of their contents. (emphasis supplied)

---

[54] The authors propose the following amendments to the Revised Penal Code provisions on libel. The text in boldface signify the revisions proposed by the authors.

Article 353. Definition of libel. —

A libel is public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead.

Article 354. Requirement for publicity. — Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown.

x x x

Article 355. Libel, means by writings or similar means. — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means and in any kind of medium including those electronic in nature, shall be punished by prision correccional in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.

The provisions of the Intellectual Property Code, are comprehensive enough to include copyright infringement perpetrated using transmissions via the Internet, whether it is coursed through *"wire or wireless means."* This would cover connections using either telephone wires, fiber optic cables, or satellite radio waves.

b. Electronic commerce/consumer protection

Certain provisions of the Consumer Act of the Philippines could find application in cyberspace.

> **Article 4. Definition of terms.** – For purposes of this Act, the term:
> a) "Advertisement" means ... any form of mass medium, subsequently applied, disseminated, or circulated advertising matter. (emphasis supplied)
>
> x x x
>
> m) "Consumer" means the sale, lease, exchange, traffic or distribution of goods, commodities, productions, services or property, tangible or intangible ... "Mass Media" refers to any means or methods used to convey advertising messages to the public such as television, radio, magazines, cinema, billboards, posters, streamers, hand bills, leaflets, mails, and the like. (emphasis supplied)
>
> **Article 110. False, Deceptive, or Misleading Advertisement.** – It shall be unlawful for any person to disseminate or to cause the dissemination of any false, deceptive, or misleading advertisement by Philippine mail or in commerce by print, radio, television, outdoor advertisement, or other medium for the purpose of inducing or which is likely to induce directly or indirectly the purchase of consumer products or services. An advertisement shall be false, deceptive, or misleading if it is not in conformity with the provisions of this Act or if it is misleading in a material respect ... (emphasis supplied)

The provisions of the Consumer Protection Act are crafted to cover any act inimical to the legal rights of the consumer which are committed *"in any form of mass medium."* *"Mass medium"* is defined as any means or methods used to convey advertising messages to the public. This is broad enough to

include electronic commerce — the sale, lease, exchange, traffic, or distribution of goods and services through the Internet.

3. Analysis and identification of problem areas in State regulation

With regard to the application of user privacy agreements, a problem arises when *highly private news groups*, under highly private contracts set by their respective system operators, send messages to users under contracts with less privacy rights. In such a case, the highly private message originates from a source where the operator is not allowed to view such information and ends up in a place where the operator is free to disclose the contents of the message. In fact, these messages can be publicized legally by the provider at any time.

Another problem area is the control of spamming. To extend more protection to both the provider and the user is allowing the former to bar "spam" or unwanted batches of commercial messages from their systems. In at least two cases in the United States involving CompuServe[55] and American Online,[56] the federal courts ruled that a dominant provider is a purely private entity and thus may bar any message from any source it does not wish to transmit. It rejected the claim of the spammer — Cyber Promotions, Inc. — that the two providers were akin to common carriers which cannot discriminate. Therefore, if a user can be found to be a trespasser, or one who engages in wrongful or tortious conduct, the courts can issue an injunction without touching on the issue of free speech.

Internet libel law is another area where there is a lack of both foreign and local legislation. In Internet communications, it can be almost impossible to determine who is really the source of a libelous message. Unlike in ordinary, non-Internet related, libel cases, it is not easy to identify who made or is responsible for posting a certain type of communication on the Internet. In fact, any person can post libelous messages on Internet sites, newsgroups, or chat rooms without identifying themselves or by using fictitious names. Even if the source is indicated in the posting, it is possible that it was done by another person who used the name of the purported source. This has been the

---

[55] Compuserve Inc., v. Cyber Promotions, Inc., 962 F. Supp. 1015 (1997).

[56] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (1996).

subject of the leading U.S. case of *Zeran v. America On-line.*[57] In this case an unknown user of the America On-line service provider posted messages that implied that Zeran was selling merchandise with highly offensive messages about the Oklahoma City bombing, such as "Finally a day care that keeps the kids quiet — Oklahoma, 1995."[58] After complaining to the provider, the posting was removed. However, this was replaced by a more severe message. What the offended party did was to sue the provider for negligence in allowing a defamatory message to appear and stay where it could cause the user great harm. The court dismissed the claim because of a provision in the Communications Decency Act which absolves providers of liability for material they did not originate and for which they are not otherwise responsible. This shows that in the United States most victims of on-line libel may lack legal recourse against any one. In the Philippines, there is likewise no clear statutory protection in cases of this nature, except perhaps for civil damages under the general provisions of the Civil Code on Human Relations[59] and Quasi-Delict.[60] If there is a contractual agreement between the offended party and his service provider regarding the posting of messages affecting the user, then the latter can have recourse under such contract.

In case the source of the libelous matter cannot be identified, the law must allow for a recourse against a negligent service provider who allows such posting to be maintained in its system. Thus liability must be imposed where the Internet service provider has the capacity to remove the offending

---

[57] 958 F. Supp. 1124 (1997).

[58] Robert M. O'Neil, *Free Speech on the Internet: Beyond "Indecency,"* 38 JURIMETRICS 617, 622 (1998).

[59] Article 19. Every person must, in the exercise of his rights and in the performance of his duties, act with justice, give everyone his due, and observe honesty and good faith.

Article 21. Any person who willfully causes loss or injury to another in a manner that is contrary to morals, good customs or public policy shall compensate the latter for the damage.

Article 33. In cases of defamation, fraud, and physical injuries a civil action for damages, entirely separate and distinct from the criminal action, may be brought by the injured party. Such civil action shall proceed independently of the criminal prosecution, and shall require only a preponderance of evidence.

[60] Article 2176. Whoever by act or omission, causes damage to another, there being fault or negligence, is obliged to pay for the damage done. Such fault or negligence, if there is no pre-existing contractual relation between the parties, is called a quasi-delict and is governed by the provisions of this Chapter.

material, but neglects to do so for an unreasonable period of time after being informed by the offended party of the defamatory or damaging message.

In the area of law enforcement, although the State can legally compel the provider to perform the interception itself through a valid judicial search warrant, the provider has a reasonable expectation that its company will not become an instrumentality of the law enforcement agency. Thus, the government should adopt the practice that no enforcement agency or official shall attempt to force any provider to make its premises available for interception of messages. Existing technology will allow the government to access the system of the provider from a remotely located computer by giving their access code to the government.

B. The passive State — self-regulation by Internet users and service providers

1. Blocking undertaken by the service provider

One method of self-regulation to prevent access that may be set up is private identity blocking. This is done through the initiative of the service provider that now has the technology to block what it deems as objectionable material, whether it be pornography, promotion of immoral doctrine, racism, or any posting tending to promote criminal activity.[61] For instance, if a provider sees a pornographic website of a domestic or foreign user, it can effectively prevent its subscribers from accessing said site. In the Philippines, blocking by the provider of a specific objectionable posting has happened at least once, when nude pictures of Philippine actresses were posted in a website. The provider blocked the site in response to the public clamor that developed against the posting. When the owner of the website applied to other providers for a new website to carry the same content, the providers rejected his application.

[61] According to Carlo Linga, system administrator of NewGen, an affiliate system provider of the Informatics Computer Institute, the provider has the means to block data coming in from sources outside its own network.

2. Express filtering

a. Filtering software

Filtering solutions are designed to facilitate content filtering through third parties who rate the content to be filtered.[62] This filtering system is initiated by private companies who sell filtering software that compiles lists of sites which the "parents" or users do not want their children to have access to, like sites dealing with the subject of sex, gambling, violence, or drugs. Only those who need filtering buy the software. It is the adult who chooses which filter software brand to buy.

The filtering approach involves the creation by the software company of a database of undesirable Internet sites contained in the filtering program. The software allows access to the Internet except to those sites the software developer deems offensive.[63] Filtering programs block web pages in two ways. One method is by searching for key words. The other method is by an examination of individual sites and the creation of a list of what sites are desirable and what are not.

b. The Platform for Internet Content Selection (PICS)

PICS is a proposed Internet language that will enable classification or labeling of websites as to content. The system was developed by the World Wide Web consortium based in the Massachusetts Institute of Technology. It would allow individuals and organizations to add descriptive labels to newsgroups and web sites and the other information offerings of the Internet.[64] PICS grew out as a reaction of the private sector to the move by the government, culminating in the Communications Decency Act, to legislate "decency" on the Internet. The group will not carry out the ratings but it will

---

[62] Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS 629, 652 (1998).

[63] Some of the Internet content filtering software available in the market are Cyber Patrol, Cybersitter, InterGo, and NetNanny. A number of these programs, aside from preventing access to undesirable sites, also prevent children from sending out personal information about themselves to chat groups or other unwanted sites.

[64] Herb Brody, *Toward a Cleaner, Tidier Net, Platform for Internet Content Selection*, 99 TECHNOLOGY REVIEW 11 (1996).

create a language or uniform format with which anyone else might create such labels. Any interest group or commercial ratings company can make its own rating list. Those who create the sites can label their own materials by inserting a code in the header that accompanies his postings. The label usually describes the extent of profanity, levels of nudity, degrees of violence, and other parameters.[65] The labeling can also be done by the service providers of the sites hosting the web page. Individuals are free to select the ratings list which he or she thinks best according to his or her preferences and values. Software developers, on the other hand, would create the filtering programs to implement the ratings. When a user accesses a website or a newsgroup, the header containing the label is first read by the user's computer. The filtering software then would scan the content and if the category is unacceptable according to the standards set by the user, the software would block the connection.

3. Analysis of problem areas and deficiencies of self-regulating schemes

Blocking and filtering are subject to limitations and only address some of the concerns that exist on the Internet, more specifically obscenity, libel and promotion of immoral/illegal acts or doctrines, and postings which promote lawlessness and mayhem in general. However, these private sector initiatives to self-regulate the Web are severely inadequate in addressing the above issues and are wholly incapable of providing a system for the enforcement of the laws against other criminal activities made through or facilitated by the Internet. In express blocking, it is the provider which decides for the user what are objectionable and what are not. The blocking done by filtering companies would necessarily reflect the ideological bias and value systems which may not be shared by the individual user.

Filtering suffers from its inherent limitation of having to use very general search criteria which almost always prevents access to an otherwise acceptable communication while at the same time failing to bar all the undesirable materials. Some filtering software simply depend on simple text recognition to bar controversial words. Others have more context sensitive

---

[65] Geofrey Ramos, *What You Can and Can't Get Away With Online*, PC WORLD 34 (October 1996).

search engines. Still there are significant shortcomings in filters. There is no simple way to check if websites are filtered in accordance with the desires of the subscriber.[66] For example, some filters excluded those sites which criticize filtering technology; also sites providing a medical discussion of AIDS are excluded because of mistaken association with obscenity.

The problem with PICS is that it cannot guarantee that the source of the content will label it truthfully or accurately. Likewise, PICS can allow state censorship as well as individual censorship. The filter can be imposed at the level of the personal computer of the user or at the level of the Internet service provider or it could be centrally controlled by the national government.

IV. THE INTERNET AND CONSTITUTIONAL VALUES

> *Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home ... Can it be that the Constitution affords no protection against such invasions of individual security?*[67]

A. The Internet as a completely novel form of communication

1. Speech and the Internet

Communication via the Internet may be considered similar to speech in the sense that both a "user" and a listener could choose to react or not to react to what they have accessed or heard. In oral communications though, a message will only reach those who are within hearing distance. On the other hand, a message sent via Internet may reach users situated halfway around the world. Even if a speaker uses a mechanism to ensure a wider audience, it does not compare to the spectrum of possible recipients in the Internet.

---

[66] For example, some filters excluded those sites which criticize filtering technology; also sites providing a medical discussion of AIDS are excluded because of mistaken association with obscenity.

[67] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

The choice of topics in oral communication is limited to the capability of the speaker. On the other hand, users of the Internet may find the sheer volume and variety of information available overwhelming. Added to this is the fact that almost a thousand new websites are created every day.[68]

2. Print and the Internet

There is only one similarity between the Internet and print media — the absence of prior restraint. Applying such a stricture on the Internet would be intimidating. The 75 million users of the Internet can be considered as possible makers of websites.[69] Monitoring these users is beyond the capability of present technology and human limitations. The contents of a newspaper though are subject to the control and supervision of an editor-in-chief. In the Internet, there is no such editor-in-chief. The website creators are free to construct Web pages with little or no supervision at all.

3. Broadcast and the Internet

The case of *Federal Communications Commission v. Pacifica* rationalized the imposition of the strictest of standards on broadcast media:

> Of all the forms of communication, broadcasting has the most limited First Amendment protection. Among the reasons for specially treating indecent broadcasting is the uniquely pervasive presence that medium of expression occupies in the lives of our people. Broadcasts extend into the privacy of the home and it is impossible completely to avoid those that are patently offensive.[70]

Both the Internet and broadcast media are indeed pervasive. All those who possess the necessary equipment (i.e. televisions, radios and computers) receive information so transmitted. Yet, as between the two media, the Internet receives the greater degree of protection. In the *Reno* case, the U.S. Supreme Court upheld the finding of the Pennsylvania District Court that

---

[68] James Martin, *Internet Overload: Disaster in the Making*, PC WORLD 145 (October 1996).

[69] See *StatMarket — Accurate Internet Statistics and User Trends in Real Time — A WebSite Production* (visited 20 February 1999) <http://www.statmarket.com/>.

[70] 438 U.S. 726 (1978).

broadcasting is more "invasive" than the Internet.[71] While communication through broadcasting is heard on the radio or seen on television screens unsought, information which appears on an Internet user's screen is a matter of his or her choice.

B. Constitutionality of regulations in cyberspace

1. Freedom of expression

> "No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances."[72]

The above-quoted constitutional provision guarantees the freedom of each individual to free expression. Expression may be in any form — speech, writings, movements or pictures. Said freedom ensures a free trade in ideas.[73] An exchange of ideas, without any kind of state-imposed restraint, is necessary to a democratic society. However, this freedom is not absolute. The State, in its exercise of its police powers, may regulate certain forms of expression in the interest of the public. Thus, expressions which are offensive to public order or morality do not deserve the protection of the state.

The State ensures such protection in two ways. The first is via prior restraint or the imposition of restrictions before the publication or dissemination of the utterance.[74] The second method of limiting the freedom of speech is by subsequent punishment. The author or creator may be held liable under the law after a judicial determination. The standards by which the courts have validated these laws against have evolved over time.

---

[71] Reno v. ACLU, 929 F. Supp 842 (1996).

[72] CONST. art. III, sec. 4.

[73] Abrams v. US, 250 U.S. 616, 670 (Holmes, J., dissenting) (1916).

[74] This kind of restriction is inapplicable to the Internet because there are 36,783 websites in existence as of February 20, 1999 and almost 1000 pages worth of information are added everyday worldwide. See *StatMarket*, *supra* note 69. To monitor such production would be asking the impossible from the state.

a. Content based standards

i. Dangerous tendency test

By this test, the State is allowed to prohibit expressions which create a dangerous tendency which the State has the right to prevent. Our Supreme Court adapted this test in the case of *Cabansag v. Fernandez*,[75] holding that "it is sufficient if the natural tendency and probable effect of the utterance be to bring about the substantive evil which the legislative body seeks to prevent." It is not necessary that the utterance actually creates the evil for a mere tendency to cause such evil is enough.[76] Two elements are to be considered in this test: the expression itself and the substantive evil which is to be determined by the legislature. If there is reasonable connection between the speech and the substantive evil, then the State can validly prevent such an expression.

Web sites originate from different states. What one state may consider as undesirable could be deemed acceptable by other states. These differences in the perception of substantive evil will render the uniform application of the dangerous tendency test impossible.

ii. Clear and present danger test

The most libertarian of all standards was expressed thus by Justice Oliver Wendell Holmes, Jr. in the case of *Schenck v. United States*:[77] "[T]he question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that the State has a right to prevent."[78] He also opined that it is a question of "proximity and degree."[79]

Our own Supreme Court has ruled that there must be a "causal connection" between the utterance and the danger of the substantive evil. The

---

[75] 102 Phil. 152, 163-164 (1957), citing Gitlow v. New York, 268 U.S. 670, 671 (1925).

[76] ISAGANI CRUZ, CONSTITUTIONAL LAW 205 (1995).

[77] 249 U.S. 47 (1919).

[78] Schenck v. U.S., 249 U.S. 47 (1919).

[79] Schenck v. U.S., 249 U.S. 47, 52 (1919).

term "present" refers to the time element. The danger must not only be probable but likely inevitable.[80]

The *Schenck* decision laid stress on the circumstances in which the expression was made. The implication is that words in themselves may not be dangerous. As applied in cyberspace, an author of a website, within the confines of his home, may create a website which, at the time and place it was made, is innocent. However, if the website was accessed by a user in another state, the same innocent material may be restricted under the clear and present danger test. The user's state may be under the state of war and the same material may threaten national security. The distance between the creator and the user in cyberspace may render the clear and present test obsolete and inapplicable.

iii. Balancing of interests test

In the case of *Gonzales v. Comelec*,[81] the Supreme Court, citing *American Communications Association v. Douds*,[82] described the balancing of interest test:

> When particular conduct is regulated in the interest of public order, and the regulation results in an indirect, conditional, partial abridgement of speech, the duty of the courts is to determine which of the two conflicting interests demands the greater protection under the particular circumstances presented.[83]

The crux of this test is the balancing of two competing interests and the determination of which is the more important and thus, entitled to protection. This test, however, cannot find constant application in cyberspace. A web page, accessible globally, cannot seek global protection under this test. Different states perceive the same value diversely. The result would be that the same web page may find protection in some states but not in others.

---

[80] Gonzales v. COMELEC, G.R. No. L-28196, 9 November 1967, 27 SCRA 835, 861.
[81] Gonzales v. COMELEC, G.R. No. L-28196, 9 November 1967, 27 SCRA 835, 861.
[82] 268 U.S. 652 (1925).
[83] Gonzales v. COMELEC, G.R. No. L-28196, 9 November 1967, 27 SCRA 835, 861.

b. Content neutral test

The previous standards consider the character of the writing in question. Regulating the kind of information available in cyberspace is a daunting task. However, a workable solution may be made if in our jurisdiction, our courts would still apply these standards if the writing itself is made available to users within this country. The courts may decide if such website is protected. If it is decided that such website an example of unprotected speech, then the courts may restrict access to such a website to users situated in the Philippines.

The U.S. Supreme Court has formulated another standard which does not take into account the composition of the writing. The case of *United States v. O'Brien*[84] validates a government restriction if it is within the constitutional power of the government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction is no greater than is essential to the furtherance of that interest.

Our Supreme Court heeded this decision in the case of *Adiong v. COMELEC*[85] when it pronounced, in effect, that there must be a substantial government or public interest in order that restrictions on an individual's freedom may validly be made.[86]

Like the content based tests explained above, this content neutral test would be difficult to apply in cyberspace. The decisive factor in this instance is the substantial governmental interest to be protected. Inasmuch as cyberspace transcends territorial boundaries, the application of this test would lead to confusion as to what these interests are.. In some situations, an interest of one state may conflict with that of another state.

---

[84] 391 U.S. 367 (1968).
[85] Adiong v. COMELEC, G.R. No. 103956, 31 March 1992, 207 SCRA 712.
[86] Adiong v. COMELEC, G.R. No. 103956, 31 March 1992, 207 SCRA 712, 718.

c. Unprotected speech: Obscenity and the community standards test

> It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interests in order and morality.[87]

Content based and content neutral standards involve a comparison of competing values. Obscenity though does not advance any social value at all. Content based and neutral standards find no application in instances involving obscenity.

Even if obscenity has been prevalent in cyberspace, no individual in this country has been punished under our penal laws for obscenity.[88] Although "cyberporn" accounts for less than five percent of all electronic traffic,[89] the fact remains that any one connected to the Internet, even a minor, can easily access these sites and print the same on paper if they chose to do so. Moreover, anyone can create a website containing obscene materials with impunity and escape penal sanctions by either creating the site in a jurisdiction where obscenity laws are lax, or by keeping his identity in the Internet unknown.

---

[87] Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

[88] REV. PEN. CODE (Act No. 3815, as amended) art. 201. *Immoral doctrines, obscene publications and exhibitions, and indecent shows.* - The penalty of *prision mayor* or a fine ranging from six thousand to twelve thousand pesos, or both such imprisonment and fine, shall be imposed upon:

(1) Those who shall publicly expound or proclaim doctrines openly contrary to public morals;

(2) (a) The authors of obscene literature, published with their knowledge in any form; the editors publishing such literature; and the owners/operators of the establishment selling the same;

(b) Those who, in theaters, fairs, cinematographs or any other place, exhibit indecent or immoral plays, scenes, acts or shows, it being understood that the obscene literature or indecent or immoral plays, scenes, acts or shows, whether live or in film, which are proscribed by virtue hereof, shall include those which: (1) glorify criminals or condone crimes; (2) serves no other purpose but to satisfy the market for violence, lust or pornography; (3) offend any race or religion; (4) tend to abet traffic in and use of prohibited drugs; and (5) are contrary to law, public order, morals, good customs, established policies, lawful orders, decrees and edicts;

(3) Those who shall sell, give away or exhibit films, prints, engravings, sculpture or literature which are offensive to morals

[89] Meyer, *supra* note 46, at 59.

The Supreme Court decided on the issue of obscenity only in three instances. In the case of *People v. Kottinger*,[90] the Court borrowed from United States jurisprudence when it stated that obscenity may be defined as meaning something offensive to chastity, decency, or delicacy. This definition is rather broad. The later case of *People v. Go Pin*[91] attempted to narrow down this definition by saying, in effect, that obscenity is an expression lacking social redeeming values. This concept was reiterated in the case of *People v. Padan*.[92]

The surfeit of American jurisprudence on the matter would be helpful in discerning obscenity in the Internet. Of a number of United States Supreme Court cases, *Miller v. California*[93] laid down the test in determining obscenity, thus:

> The basic guidelines for the trier of facts must be: (a) whether the 'average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest...(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[94]

It is interesting to point out that the first prong of the *Miller* test stressed the application of "contemporary community standards."[95] Again, the question arises as to *which* community is to be taken into account if this test were to be applied to the Internet. It seems that the three-pronged *Miller* test would be at odds with the global character of the Internet. Is the whole world to be considered as a single community? The answer would be in the negative. An attempt to consolidate values of different nations in order to come up with

---

[90] 45 Phil. 352 (1923).

[91] 97 Phil. 418, 419 (1923). "[The] supposed artistic qualities of the said picture were being commercialized so that the cause of art was of secondary or minor importance. Gain, not profit, appeared to be the main, if not exclusive consideration in the exhibition."

[92] 101 Phil. 749 (1957).

[93] 413 U.S. 15 (1973).

[94] Miller v. California, 413 U.S. 15, 124 (1973).

[95] Miller v. California, 413 U.S. 15, 124 (1973).

contemporary community standards would raise discord among opposing points of view.

The United States Congress attempted to codify through the Communications and Decency Act existing jurisprudence regarding obscene or indecent materials being sent through any telecommunications facility, including the Internet. The community standards test, as enunciated in *Miller*, was applied in the Communications Decency Act.[96] However, the United States Supreme Court stated in *Reno v. ACLU*[97] that the statute in question was both vague and overbroad. The Court took note of the three-prong *Miller* test. According to the Government, the CDA is valid insofar as it only codified jurisprudence, more specifically the community standards test in *Miller*. The Court was not persuaded by this argument for the reason that the second prong of the *Miller* test requires that the proscribed conduct be also specifically defined by the applicable state law. The CDA did not specify the prohibited acts but described these acts as either "obscene" or "patently offensive."

The American justices virtually gave the Internet the highest level of protection. It is highly improbable that Philippine courts will decide in the same light as the *Reno* case. It seems that the concept of socially redeeming values vis-à-vis the obscene material will remain the standard by which Philippine courts will decide. Moreover, the Revised Penal Code, article 201, may well cover obscene materials available on the Internet and accessible by those having computers within the Philippines. To be exact, creating a website containing pornographic materials can be considered a violation either of article 201, paragraph (1) for being an act publicly expounding or proclaiming

---

[96] (d) Whoever — (1) in interstate or foreign communications knowingly —
(B) uses any interactive computer service display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communications; ... shall be fined under Title 18 or imprisoned not more than two years or both.

[97] Reno v. ACLU, 117 S.Ct. 2329 (1997).

doctrines openly contrary to public morals, or of article 201 paragraph (3) for selling, giving away or exhibiting of literature which is offensive to morals.[98]

Nevertheless, a problem would arise if the material adjudged to be obscene proceeded from a creator in another jurisdiction. Philippine penal laws cannot transcend territorial and political boundaries. A paradox arises: the Philippines can prosecute under the Revised Penal Code but we cannot punish the criminal.

The Federal Republic of Germany may serve as an example for future action. In December 1996, over 200 websites were determined to contain sexual materials prohibited by the law. The law enforcement agencies requested the servers to stop from sponsoring such websites. When the servers refused, German authorities blocked communication of users within Germany to the server. Until the server complied with the order of the German courts, its websites remained inaccessible.

This plan of action is feasible since technology allowing the blocking of access to selected websites is already available. However, to cut off access to websites not otherwise objectionable under Philippine obscenity law would be a violation of the constitutional right to free speech. A modification of the German action is in order. Local law enforcement agencies can only prevent access to and from specified sites.

2. Privacy in cyberspace

> The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.
>
> Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.[99]

This provision implies that every individual is entitled to his or her secrets. Again, this privilege is not absolute for the provision states exceptions:

---

[98] REV. PEN. CODE art. 201.

[99] CONST. art. III, sec. 3, par. (1).

public safety or order. These two concepts are open to broad interpretation and application; hence, the framers of the Constitution, in order to prevent abuses of this exception, provided that such intrusion to an individual's privacy must be prescribed by law.

The introduction of the Internet into the daily lives of its users presented unprecedented problems with regard to privacy. Although "e-mail" is very popular nowadays due to its speed, efficiency and economy, it can still be subject to prying eyes of unscrupulous individuals. One way to protect the privacy of Internet users is for the State to impose penal sanctions on intruders, both private and governmental entities. The State can consider any evidence of a crime available on the Internet to be inadmissible in all instances.

On the other hand, imposing laws strictly protecting the privacy of the user may unnecessarily tie the hands of governmental agencies. The Internet is available to everybody, hence, anything can happen in cyberspace. Using the Internet for committing crimes is not unusual. For instance, one may engage in "virtual gambling"[100] although prohibited in this jurisdiction, or the selling of illegal drugs on the Internet. One reason why the Internet is considered a haven for criminal activity is the fact that the criminals themselves can mask their identities. Furthermore, they cannot be apprehended because e-mail addresses and websites do not correspond to real addresses.

a. Reasonable expectations of privacy of Internet users

The determination of the scope of privacy is important in order to limit valid governmental intrusion into such right. There is no definitive concept of privacy in our jurisdiction, that is, the courts have not yet drawn the line as to where state intrusion will become unconstitutional. The U.S. Supreme Court, in *Katz v. United States*,[101] introduced the concept of reasonable expectation. The Court laid down a two-pronged test for allowing state intrusion: (1) if the government action has violated an individual's subjective expectation of privacy; and (2) if society recognizes such expectation

[100] Meyer, *supra* note 46 at 61.
[101] 389 U.S. 347 (1967).

as reasonable.[102] As applied in traditional communication, a person who sends a letter through mail can reasonably expect that said letter will not be opened and read by persons other than the intended recipient. If such reasonable expectation exists, then the State cannot intrude in such matters. Conversely, if a person sends a postcard, he or she cannot reasonably expect that others will not read the message written thereon.

In effect, the reasonable expectation test stresses the importance of the modality used by the sender in communication. The susceptibility of interception becomes a factor which ascertains the reasonableness of the sender's expectation. As the technology in the field of electronic communication progresses, the susceptibility of interception also increases. Similarly, developments in other fields of technology in the real world decrease the reasonable expectation of individuals. For instance, before the advent of X-ray technology, a person other than the sender or recipient would not be able to discern the contents of a sealed package. With the use of X-ray machines, individuals can now see the contents of the same package.

There are some steps which can be taken by users in order to protect their privacy. These are:

1. *There must be an agreement between the service provider and the user as to the degree of privacy the former accords the latter.* In this country, there is no written contract enumerating the rights and duties of both the user and the provider. Without such a written contract, only a moral obligation prevents the provider from intercepting communications from the user. If the privacy of communication of the user is not expressly stipulated, nothing can stop the provider from reading such communication. If no prohibition exists on the part of the provider, he may very well consent to a search of the user's communication by law enforcement agencies. In such a situation, the constitutional right of the user against unreasonable search is violated.

2. *The communication must be protected by the user himself.* Before sending a communication, the user must take measures to ensure that it would not be intercepted by persons other than the intended recipient. The user can

[102] Katz v. United States, 389 U.S. 347, 353 (1967).

protect his communication by means of a password that only he and his recipient knows. If somebody else bypasses or breaks the password, then such intrusion would be a violation of the user's right to privacy. Another measure the user can undertake is encrypting the communication. However, encryption does not ensure complete privacy because there are deciphering software available in the market. Decryption unauthorized by the user may be used in such a way that it does not violate the Constitution. In a case decided by a United States Court, the translation of a communication in another language into a language understood by law enforcement personnel was allowed.[103] Decryption technology may develop in such a way that deciphering is regularly used. Hence, this kind of method may be effective today, but not in the future.

b. The Anti-Wiretapping Law (Republic Act No. 4200)

The Anti-Wiretapping Law seeks to protect the privacy of communication by penalizing those persons who tap into private communication or spoken word without the consent of all parties.[104] Although such protection is broad enough to include communication via the Internet, the means by which the tap is made is limited (i.e. dictaphone, dictagraph, detectaphone, or walkie talkie). By the principle of *ejusdem generis*, the phrase "however otherwise described"[105] should be construed to mean that other means by which a communication may be tapped should be of the same import as the ones enumerated. This law though was enacted way back in 1965, and is now outdated. In order that the right to privacy be properly protected in light of the advances in Internet technology, a new law must be drawn in order to adapt to such advances. Moreover, the list of crimes for which a court order authorizing wire-tapping will issue is limited to crimes against national security (i.e. treason, rebellion, sedition, etc).[106]

---

[103] United States v. Truong Dinh Hung, 629 F.2d 908, 916-917 (1980).

[104] Rep. Act No. 4200 (1965) sec. 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or hear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or detectaphone or walkie-talkie or tape recorder, or however otherwise described....

[105] Rep. Act No. 4200 (1985), sec. 1.

[106] Rep. Act No. 4200 (1985), sec. 3.

The ECPA defined electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence on any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[107] As compared to our Anti-Wiretapping Law, this definition covers a wide variety of communication and also reflects the advances made in communications technology. Needless to say, communication via Internet falls under this definition.

Offenses for which an interception may be authorized under ECPA by a court cover a wider range than our Anti-Wiretapping Law. For instance, crimes related to trafficking of certain motor vehicles, fraud, and racketeering are included.[108]

Noticeable in the ECPA is the specification given to offenses involving access to stored communication. It punishes whoever "intentional[ly] accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds that authorization given."[109] This provision clearly protects the integrity and privacy of communications via Internet. It specifically applies to interceptions made by persons other than the sender or the intended recipient. No provision of this import is included in the Anti-Wiretapping Law.

3. Searches and seizures in cyberspace

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to searched and the persons or things to be seized.[110]

---

[107] *See* ECPA, Pub. L. No. 99-508, § 101(a)(b)(c), (1986) (codified as amended at 18 U.S.C. § 2510(12)).

[108] *See* ECPA, Pub. L. No. 99-508, § 105(a)(1), (1986) (codified as amended at 18 U.S.C. § 2516(1)).

[109] *See* ECPA, Pub. L. No. 99-508, § 201, (1986) (codified as amended at 18 U.S.C. § 2701 (a)).

[110] CONST. art. III, sec. 2.

This constitutional provision upholds the inviolability of an individual's home. It is divided into two parts: (1) the right of persons against unreasonable searches and seizures; and (2) requisites for a valid search or arrest warrant. Implied therein is the possibility of conducting a warrantless search which is not illegal.

a. Searches with warrants

The court order required in order to intercept or tap a private communication under the Anti-Wiretapping Law is similar to a search warrant. The judge issuing the order must examine under oath the applicant and the witnesses he may produce. The order will issue only upon finding reasonable grounds to believe that the crime so specified has been committed or is about to be committed.[111] However, these orders differ from search warrants in one respect. While there is a requirement that there be a particularity of description of the items to be seized in search warrants, there is no such need under the Anti-Wiretapping Law. Under the said law, all the order must include are: (1) the identity of persons whose communication is to be intercepted or recorded; (2) the identity of the officer who will conduct the interception or recording; (3) the offenses committed or sought to be prevented; and (4) the period of authorization which must not exceed sixty days.[112]

On this matter, the ECPA is more stringent in the sense that the officer applying for the order must specify the facility from which communications are to be intercepted.[113] This requirement only applies to wire or oral communication.

b. Allowable warrantless searches

There are four kinds of warrantless searches allowed under our laws: (1) searches incidental to an arrest; (2) search of moving vehicles; (3) customs searches; (4) search done under the plain view doctrine.

---

[111] Rep. Act No. 4200 (1965), sec. 3.
[112] Rep. Act No. 4200 (1965), sec. 3.
[113] *See* ECPA, Pub. L. No. 99-508, § 106(d), (1986) (codified as amended at 18 U.S.C. § 2518(1)(b)).

Of the four types of allowable warrantless searches, a search done *in plain view* finds significance in cyberspace. The "plain view doctrine" was first expounded in the case of *Harris v. United States*:[114] "[O]bjects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence." The Supreme Court has applied this doctrine in several cases which usually involve drug possession.[115]

There are two views on the applicability of the plain view doctrine in cyberspace. The first view posits that all information available on the Internet is actually in plain view of a peace officer. This is because all websites are easily accessed by anyone. Thus, to say that an officer of the law is precluded from using information culled from the Internet is untenable.[116]

The second view puts forward the theory that anything seized from the Internet is inadmissible for the simple reason that whatever a user might access is never "inadvertent."[117] The act of entering keywords and engaging the search engine to look for information related to the subject of inquiry is already an intentional act.

Of the two views, the second is preferred. The Constitution clearly prohibits unreasonable searches and seizures. An officer browsing through the Internet, with the intention of capturing criminals and gathering evidence, is actually conducting a fishing expedition. At the moment he types in the subject of inquiry, he does not know who the perpetrator is or that a crime has happened at all. For all he knows, his search may produce no possible websites.

The anonymity accompanying Internet usage may be a huge stumbling block to law enforcement authorities. Criminals might find cyberspace their

---

[114] 390 U.S. 294 (1968).

[115] *See* Roan v. Gonzales, G.R. No. L-71410, 25 November 1986, 145 SCRA 687, 697. *See also* People v. Asio, G.R. No. 84960, 1 September 1989, 177 SCRA 250, 256.

[116] Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1608 (1997).

[117] Coolidge v. United States, 403 U.S 472 (1971).

haven. On the other hand, users have the right to be secure from unreasonable searches and seizures.

A compromise may be reached between these two competing interests. The State may easily provide a procedure for the issuance of search warrants or interception orders specifically applicable in cyberspace. The procedure laid down in both the Anti-Wiretapping Law and the ECPA is enough to satisfy both interests.

V. IMPLEMENTING STATE REGULATION OF THE NET

It has been said that the best government that which governs the least. Self-regulation by mature Internet users seems to be an ideal solution. It seems inescapable, though, that at least in the short-term the Philippine government will sooner or later join the list of countries that actively intervene in the Internet.

A. State monitoring of Internet communications

Two of the special concerns in the Internet are the security and privacy of communications. Messages which are directed to a final destination normally pass through several systems and networks which are operated by government agencies or private individuals or groups. The ECPA was passed to balance the privacy and security interests of the individual or entity vis-à-vis the legitimate law enforcement needs of the government. However, in the Philippines, even a long-time Internet user may not be aware that his or her electronic mail can be read easily by the employees of the system provider. There is now technology which allows an eavesdropper or a technician monitoring an Internet router[118] to scan the contents of electronic mail and other Internet data transmissions for preprogrammed words or phrases.

Legal state monitoring of Internet transmissions under a statute like the ECPA is now very easy. According to Carlos Linga of NewGen, Inc.,

[118] Comment, *Privacy and Encryption in Cyberspace*, 34 SAN DIEGO L. REV. 1401, 1404 (1997). A router is a piece of computer hardware that directs the flow of traffic across computer networks. When messages are sent via the Internet, the routers send the message through the routes with the least congestion. The sender of the message has no control over the path through which the message is sent.

there are two ways by which law enforcement authorities can tap Internet communications with suspected illegal content or messages used to carry out and facilitate criminal activity. On-site interception or access could be done by law enforcers by intercepting a real-time transmission or accessing a message stored in the system of the provider using the provider's computer system in the latter's office or station. Off-site interception or access is done by first requesting the access code of the provider's system and then connecting it to the law enforcement agency's computer. This functions like a remote computing service wherein the law enforcer can do the surveillance right in his own office as if he were in front of the provider's system. Without the access code, the law enforcement agency cannot gain access to the provider's system. As unauthorized access by government hackers is a danger that the provider faces, the law must extend to the provider a measure of protection by giving it the right to sue civilly and criminally against the guilty law enforcement officers who acted without a court order or search warrant.

B. Computerized records as evidence

It is inevitable that in the enforcement of laws and prosecution in computer-related and Internet-related crimes, computerized records are necessary and may sometimes be the only evidence that can be presented by law enforcers. Computerized records are necessary for purposes of securing search warrants directed to Internet service providers to allow the State to intercept real-time transmissions and/or access stored messages in the provider's system. Even in the presentation of proof in court for crimes committed through the use of the Internet, computerized records are vital to a successful prosecution of the case.

In the United States, the issue of admissibility of computerized records was settled as far back as 1988 in the leading case of *United States v. Bonallo.*[119] In said case, the defendant Bonallo was accused and convicted of bank fraud. It was shown that he made a "fraud program" which enabled him to make withdrawals from funds from Automated Teller Machines (ATMs). The prosecution presented computer printouts of the said program which they acquired from the computer program files in Bonallo's program library.

[119] United States v. Bonallo, 858 F 2d.1427 (1988).

Computer logs of transactions were also presented in evidence. Bonallo argued that the evidence was untrustworthy; the program was in fact made by another person, and the computer logs were altered. The court ruled that the computerized records were admissible evidence. It stated that the mere possibility that the records presented may have been altered goes only to the weight of the evidence and not its admissibility.

Our Supreme Court has also had the occasion to rule on the admissibility of computerized records in the Philippines. In *People v. Burgos,*[120] it ruled that computer printouts are admissible evidence and this is not affected by the fact that the prosecution possessed them. Such possession did not necessarily imply that it had altered or tampered with the evidence to strengthen its case. Official duty is presumed to have been regularly performed. Likewise, the Court ruled that diskettes into which data is encoded and stored are admissible. [121]

C. Jurisdiction in claims for civil damages or prosecution of crimes committed through the Internet

The Internet is a means of communication that can effortlessly and pervasively invade the forum state. A provider who makes a posting on the Internet makes it available to all users worldwide. Because of the very nature of the Internet — where a posting done in one side of the globe can reach practically the entire world — there will be many instances when the citizens of a particular state will lack available redress against out-of-state offenders who caused them injury or economic harm. This injury may arise from several possible causes like intellectual property right infringement, defamation, or product liability.

The problem of jurisdiction in Internet related cases has been a major concern in the United States. This is brought about by the federal or multi-state setup of its government where issues of personal jurisdiction by one state over the defendants belonging to another state of the union has traditionally confronted the American courts. This problem was exacerbated by the arrival

[120] People v. Burgos, G.R. No. 92739, 2 August 1991, 200 SCRA 61.
[121] People v. Burgos, G.R. No. 92739, 2 August 1991, 200 SCRA 61, 72.

of the Internet which provided another medium by which people from the different states of the U.S. can interact and have business dealings with each other.

In the Philippines, the problem of jurisdiction is less complicated since it is a single-state country. Criminal suits can be maintained against Philippine residents while civil actions for damages may be brought not only against resident individual users but also locally domiciled juridical entities (like a local Internet service provider) for violating the rights of the user. For out-of-state defendants, effective legal action can be secured in Philippine courts for civil damages only if they have properties in the Philippines.[122] Such properties can be made the subject of execution even if the defendant cannot be found in the Philippines.

D. Use of encryption/decryption technology

Another development which could either strengthen or weaken the law enforcement capabilities of the government is the use of encryption/decryption technology. Encryption is the process of changing plain text into unintelligible code. Decryption is the process of changing an encrypted message back into plain text. For decryption to be carried out, one must have the code or key[123] that corresponds to that message. Previously, the use of encryption was limited to the military intelligence community and in advance mathematics courses, but recent developments have enabled the private sector to communicate in codes which even the military may not be able to decipher.[124] Encryption gives additional security to the Internet user

---

[122] RULES OF COURT, rule 4, sec. 3.

[123] Keys refer to the encrypting and decrypting codes. There are two systems currently in use. In the single key or "symmetric system," the sender and receiver must agree before the message is sent to share the secret key. The problem with this system is how to share the encrypting/decrypting key without compromising its security. In the two key or "asymmetric system," each user has a unique pair of keys: a "public key" and a "private key." After the message is encrypted by the sender, only the holder of the recipient's private key can decrypt the message. The two key system is likened to a voice mail system. In a voice mail system, one is assigned both a phone number and a password. The phone number/mailbox number may be made known to anyone. Messages may be left by these people in the mailbox. However, only the owner of the voice mail has the password, and only he or she can gain access to the messages. See Comment, *supra* note 118, at 1402.

[124] Comment, *supra* note 118, at 1406.

that his messages will be protected from hackers or unauthorized readers. Cryptography in methods of authentication and digital signatures can prevent spoofing and message forgeries.

In the United States, law enforcement agencies are pushing for restrictions on the use and the export of encryption technology to preserve their ability to eavesdrop on electronic communications. One of these proposals has been the so-called Clipper Chip system whereby the U.S. would regulate domestic usage by using proposed key escrow systems. This will allow Internet users the use of strong encryption while maintaining the State's emergency decryption capability. This is done by linking encrypted data to a data recovery key. The data recovery key is held by a trusted fiduciary like a government agency, court, or even a bonded private organization. Law enforcement agencies seeking access need to secure a court order before they can be issued a key.

Encryption can be treated in three ways by those who operate the systems through which encrypted messages are passing:

1. *System operator allows encrypted messages to pass through the system.* This entails great risk on the part of the system operator. If law enforcers discover illegal activity going on in the system, the system can be seized as proof of the crime.

2. *System operator allows no encrypted messages to pass through the system.*

3. *System operator allows encrypted messages to pass through the system as long as the system operator is given a decryption key.* The messages of the users are secure from government intrusion yet the system operator is also protected against unknown seizures.

This is another area where a the State must strike a balance between the privacy rights of the individual and the legitimate concerns of law enforcement agencies. Without government ability to decrypt messages, the Internet can become a safe haven for criminal activity. In the absence though of a clear danger to national security brought about by the proliferation of

encryption software, the balance should tilt in favor of the protection of privacy rights of users. Moreover, any user-system provider contract should make clear their agreement with regard to the use of encryption in messages transmitted through its system.

E. Creation of a special government agency to regulate use of the Internet

In rejecting the validity of the CDA, the U.S. Supreme Court distinguished the *Reno* case from *Pacifica*:

> First, the order in *Pacifica* issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when — rather than whether — it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet.[125]

With this assertion, the United States Supreme Court perceived the need for the regulation of the Internet. Of all the administrative agencies in the United States, the Federal Communications Commission (FCC) has the expertise to carry out regulations that apply existing laws to unique communications technology. The FCC was granted by the United States Congress the power to grant and renew,[126] transfer,[127] and revoke[128] licenses of persons, firms or groups engaged in the communications business. It shall consider public convenience, interest or necessity in granting an application for a license, and also considers several other factors, such as the financial capability and character of the applicant.

In the Philippines, we have a similar body — the National Telecommunications Commission (NTC). Before a public utility can operate, it must first by granted a franchise by the Congress.[129] After such franchise

---

[125] Reno v. ACLU, 117 S.Ct. 2329 (1997).

[126] 47 U.S.C. § 307.

[127] 47 U.S.C. § 309.

[128] 47 U.S.C. § 312.

[129] CONST. art. XII, sec. 11. No franchise, certificate, or any other form of authorization for the

has been obtained, the National Telecommunications Commission (NTC) shall grant the entity a Certificate of Public Convenience and Necessity (CPCN) which shall not be shorter in duration than five years nor longer than the life of the franchise.[130] In exercising its regulatory powers, the NTC must maintain an administrative process that is stable, transparent and fair, giving due emphasis to technical, legal, economic, and financial considerations.[131] The definition of the term "telecommunications,"[132] due to its broadness, may include the Internet. As such, the Internet service providers may be also required to apply for a franchise from Congress and be under the supervision of the NTC. However, Internet service providers are not required to be registered with the NTC. All that is required is registration with the Securities and Exchange Commission.

While the Internet is not as intrusive as radio or television, it should still be regulated. Information gathered from the Internet may range from esoteric scientific formulas to mundane writings with no informative value at all. In between, there is the risk that obscene, libelous and other writings of little or no social value may also exist. Hence, there is a need for regulation. However, regulation of the website creators is impossible for they are scattered around the world. What the government can do is to regulate the Internet service providers themselves. Providers have the technical capability to restrict access to and from websites containing prohibited communication, in accordance with law. If they fail to do so, what the NTC could do to punish them is to revoke the CPCN of the provider.

---

operation of a public utility shall be granted except to citizens of the Philippines or to corporations or associations organized under the laws of the Philippines at least sixty per centum of whose capital is owned by such citizens, nor shall such franchise, certificate, or authorization be exclusive in character or for a longer period than fifty years. Neither shall any franchise or right be granted except under the condition that it shall be subject to amendment, alteration, or repeal by the Congress.

[130] Rep. Act No. 7925 (1995), sec. 16.

[131] Rep. Act No. 7925 (1995), sec. 4 par. (i).

[132] Rep. Act No. 7925 (1995) sec. 3 par. (a). Telecommunications - any process which enables a telecommunications entity to relay and receive voice, data, electronic messages, written or printed matter, fixed or moving pictures, words, music or visible or audible signals or may control signals of any design and for any purpose by wire, radio or other electromagnetic, spectral, optical or technological means.

Would the operation by the providers require the possession of a congressional franchise? One must look at the nature of Internet technology. Messages sent via Internet pass through telephone lines, and in the future, fiber optic cables used in cable television. The operators of cable television services and telephone companies are already grantees of congressional franchises. If we were to consider the Internet as a mere derivative use of telephone facilities, then there is no need for a franchise.

What our legislators can do is to authorize the NTC to grant licenses to qualified Internet service providers. The grant of said license would depend on continued observance by the provider of our laws relating to obscenity, libel, consumer protection, privacy of communications and others. Should the provider violate these laws, the NTC may sanction them by imposing a fine or by revoking its license, as the law would provide.

VI. CONCLUSION

The technologies of communication change dramatically. The law must keep pace with these developments, but it should not attempt to retard it. Instead, the law must guide its growth in order to ensure that technology will serve and not enslave or poison the public good. Society has no choice but to defend itself against unknown dangers arising from technological developments. This can be in the form of active regulation of certain aspects of cyberspace or promotion of self-regulation.

The Philippines cannot adopt a regime of laissez faire with respect to the Internet. Self-regulation (i.e. blocking, filtering, or rating) can exist side-by-side with government intervention. These are not mutually exclusive remedies. The State should encourage the further development of these self-regulatory technologies. However, self-regulation alone cannot solve or at least minimize the abuses in the use of the Internet. There appears a great need for laws which clearly criminalize undesirable activities committed on the Internet as well as legislation to provide for law enforcement in Internet-related crimes.

Legal remedies under present laws in the country are rendered obsolete because of the rapid pace of technological innovations. There is an immediate

need, at least in the short term, of enacting laws specifically directed at regulating the Internet. In law enforcement, enactment in the Philippines of a law similar to the U.S. Electronic Communications Privacy Act would go a long way in protecting the rights of the Internet user as well as in allowing the government to undertake its legitimate law enforcement activities. Likewise, minor amendments in the laws relating to libel and anti-obscenity/immorality doctrines are recommended. Regulatory agencies must be formed with the technical competence to implement the rules.

Even if a country succeeds in passing laws that regulate Internet communications by users or providers within its territorial jurisdiction, there can be no lasting solution to the problem of abuses on the Internet if nations will not coordinate with one another. After all, cyberspace has no territorial boundaries and is not subject to the control of one single authority. In the long term, it is important for the international community to convene an international summit to draft globally acceptable cyberspace principles and practices. These international principles should pertain to privacy protection, State law enforcement, jurisdiction, extradition (where records pass simultaneously through different territorial jurisdictions), and harmonization of the use of data. This should culminate in the adoption of an international treaty governing conduct on the Internet, which may be patterned after the *United Nations Convention on the Law of the Seas*. It is for everyone's interest that order prevails in cyberspace. This domain, after all, is now the battleground of the present and the future.

- oOo -