UIC John Marshall Journal of Information Technology & Privacy Law

Volume 16 Issue 4 Journal of Computer & Information Law - Summer 1998

Article 8

Summer 1998

International Internet Regulation: A Multinational Approach, 16 J. Marshall J. Computer & Info. L. 997 (1998)

Steven M. Hanley

Follow this and additional works at: https://repository.law.uic.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Steven M. Hanley, International Internet Regulation: A Multinational Approach, 16 J. Marshall J. Computer & Info. L. 997 (1998)

https://repository.law.uic.edu/jitpl/vol16/iss4/8

This Comments is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

INTERNATIONAL INTERNET REGULATION: A MULTINATIONAL APPROACH

World Wide Volkswagen¹ admonished courts to take into consideration the interests of the "several States," in addition to the forum state, in the efficient judicial resolution of the dispute and the advancement of substantive policies. In the present case, this advice calls for a court to consider the procedural and substantive policies of other nations whose interests are affected by the assertion of jurisdiction by the California court ... Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field."²

I. INTRODUCTION

Countries are concerned over the content of the information its people are exposed to by the Internet.³ For example, the United States passed the Communications Decency Act of 1996⁴ to fight pornography over the Internet.⁵ Germany forced CompuServe, Inc.⁶ to block 200 dis-

3. The Internet may be defined as:

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

Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2334 (1997).

4. See 47 U.S.C. §§ 223 (a) - (h) (1996) (United States federal legislation defining offensive material and assigning a penalty for distributing offensive material on the Internet).

5. See id. The pertinent provisions of the CDA state as follows: § 223 (a)(1)(B) (1996):

(a) Whoever -

- (1) in interstate or foreign communications
 - (B) by means of a telecommunications device knowingly

^{1.} See, e.g., World-Wide Volkswagen Corp. v. Woodsen, 444 U.S. 286 (1980) (the United States Supreme Court addressing the jurisdictional reach of a forum state when a defendant's association with the forum state is minimal).

^{2.} See Asahi Metal Industry Co. v. Superior Court, 480 U.S. 102, 115 (1987). Statement from United States Supreme Court Justice O'Connor regarding the applicability of the notion of American jurisdiction over a Japanese corporation.

cussion groups to German web sites⁷ in fear of pornography and pro-Nazi messages.⁸ France prosecuted a web site owner for uploading a book that revealed secrets about a former French president.⁹ Singapore holds both Internet users and on-line service providers responsible for keeping pornographic and politically objectionable material off the Internet.¹⁰ In an attempt to shield its people from Western influence, China plans to build an "Intra-Net" which would remove China from the Internet and replace it with a Chinese version of the Internet.¹¹

§ 223 (d) (1) - (2) (1996):

(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 an 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 an activity, shall be fined under title18, United States Code, or imprisoned not more than two years or both.

Id.

6. See M.A. PIKE, USING THE INTERNET 49 (2d ed. 1995). CompuServe Inc., is a commercial on-line service vendor. See id. Competitors of CompuServe include Prodigy, America On-line, and Delphi. See id.

7. See Reno, 117 S. Ct. at 2335. A web site or web page is information stored in remote computers which is generally available to a viewer for the viewer to communicate with a web site's author. See id.

8. See Amy Knoll, Any Which Way But Loose: Nations Regulate The Internet, 4 TUL. J. INT'L & COMP. L. 275, 288 (1996) (noting that the German government finds pro-Nazi propaganda equally as intolerable as indecent material).

9. See Banned President Mitterand Book Posted Online, Newsbytes News Network, Jan. 25, 1996, available in WESTLAW, NEWSBYTE File, (French government attempting to halt the distribution of a biography on ex-President Mitterand written by Mitterand's doctor disclosing that the ex-president failed to disclose a grave illness).

10. See McDermott, Singapore Unveils Sweeping Measures To Control Words, Images on Internet, WALL ST. J., Mar. 6, 1996, at B6 (Singapore holds both Internet users and online service providers legally responsible for keeping pornographic and politically objectionable material off the Internet).

11. See Information Technology: China Opens Up - At Last, 1997 ASIAN REVIEW OF BUS. & TECH., June 1, 1997 (stating the Chinese government allows Internet communication between the Chinese public, however, the Chinese public cannot access foreign web sites).

⁽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 18 years of age, regardless of whether the maker of such communication place or initiated the communication; shall be fined under title 18, United States Code, or imprisoned not more than two years or both.

1998] INTERNATIONAL INTERNET REGULATION

Two problems confront proponents to an international solution to Internet regulation: (1) each country¹² upholds a different standard of tolerance to "egregious" information and therefore, regulation is improbable, and (2) the nature of the Internet does not lend itself to identifying or applying conventional methods of jurisdiction upon a violator. This Comment proposes first, each country has a right when regulating the Internet to uphold its national values and customs and second, Internet Service Providers (hereinafter ISPs) shall work with each country's government to provide a level of service commensurate with the ideals of the society. First, this Comment addresses specific countries and their corresponding efforts at regulating Internet information. Second, this Comment addresses methods of Internet regulation and their respective deficiencies. Third, this Comment proposes a multinational solution for Internet regulation. The Multinational Approach to Internet regulation is two-fold. First, it facilitates a flexible regulatory structure allowing nations the freedom to employ a desired degree of regulation. Second, the Multinational Approach focuses on ISPs and a Government's control over them. Finally, this Comment concludes by advising all countries connected to the Internet to form an international committee to implement a flexible regulatory system which allows nations to exercise varying degrees of regulation over the Internet while maintaining sovereignty.

II. BACKGROUND

A. STRUCTURE OF THE INTERNET

A unique feature of the Internet is that a computer in one region of the world can access a computer in another part of the world in a matter

^{12.} See Mark Lottor, Network Wizards (last modified Jan. 1997) http://www.nw.com/. Currently, there are 176 Internet connected countries. See id. The fastest growing (over 100% growth from Jan. 31, 1996 to Jan. 31, 1997) Internet domains are:

Albania, Andora, Anguilla, Argentina, Armenia Azerbaijan, Bahrain, Barbados, Belarus, Belgium, Belize, Bermuda, Bolivia, Brazil, Bulgaria, China, Colombia, Costa Rica, Cote d'Ivoire, Croatia, Cuba, Cyprus, Czech, Denmark, Dominican Republic, Egypt, El Salvador, Estonia, Georgia, Ghana, Gibraltar, Greenland, Guam, Guatemala, Hong Kong, Hungary, India, Indonesia, Italy, Japan, Jordan, Kazakhstan, Kenya, Korea, Kuwait, Latvia, Lithuania, Luxemborg, Macau, Macedonia, Malaysia, Mexico, Moldova, Monaco, Morocco, Namibia, Nepal, New Caledonia, Nicaragua, Pakistan, Panama, Peru, Philippines, Poland, Portugal, Romania, Russian Federation, San Marino, Senegal Liechtenstein, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Swaziland, Thailand, Tonga, Trinidad, Tobega, Turkey, Ukraine, United Arab Republic, United States, Uruguay, Uzbekistan, Vatican, Venezuela. Id. Since July 1996, twenty one countries have entered including the Internet including: Barbados, Botswana, Burundi, Congo, French Guiana, French Polynesia, Guadeloupe, Guernsey, Isle of Man, Jersey, Lesotho, Maldives, Micronesia, Nigeria, Norfolk Island, Papua New Guinea, Saint Kitts and Nevis, Tanzania, Togo, Yemen and Zaire. Id.

of an instant.¹³ Furthermore, the information being sent travels in such a fashion that it is broken up into individual information transmissions called "packets." These packets travel along different paths to recombine at a destination.¹⁴ This decentralized network¹⁵ relies on ISPs¹⁶ to act as intermediaries to funnel information transmissions¹⁷ through a common node before a message reaches its destination.¹⁸ However, a vast amount of ISPs exist to maintain the Internet. Therefore, a single ISP does not have the capability of supporting the pathway for all information packets traveling over the Internet.¹⁹

Another unique, but troublesome, aspect of the Internet is the ability for the sender of a message to maintain complete anonymity.²⁰ A

15. See E. DIAMOND ET AL., THE ANCIENT HISTORY OF THE INTERNET, AM. Heritage, Oct. 1, 1995, at 9. Having a centralized information receiver to send information directly from one computer to another is most efficient, however the United States Government envisioned a complete loss of communication if an enemy destroyed the centralized system therefore a decentralized network was formed. See *id*.

16. See PIKE, supra note 6, at 49. An information service provider ("ISP") may be defined as a company with an Internet "gateway." See id. A "gateway" or "router" is a dedicated telephone line capable of facilitating high speed transmissions. Id. at 47. ISPs generally charge a flat fee for membership, however, some ISPs charge based on the amount of time a user is on-line. Id. at 49. Companies in the business of providing service include CompuServe, Delphi, America Online, and Prodigy. See id.

17. See KROL, supra note 14, at 26 (noting information transmissions or portions of the millions of messages sent via the Internet travel in the form of packets). See id.

18. Id. at 26-30. The author makes a rather effective analogy of the United States Postal Service structure to explain the otherwise complicated structure of the Internet. See id. The Internet is actually a network of sub-networks where the pieces making up the sub-networks are connected by a set of computers called routers. See id. Telephone lines or gateways are equivalent to the trucks and planes of the Postal Service. See id. Routers can be thought of as postal substations in that the substations determine how to route the information pieces or "packets." See id. Comparable to a post office receiving a letter, the post office delivers this letter to another post office where the letter awaits being sent to another post office until the letter has reached its final destination. See id. Similarly, a transmission sent from a computer divides into packets and each packet travels to separate substations until all packets reach a transfer control protocol ("TCP") which reforms the packets into the original message. See id.

19. See PIKE, supra note 6, at 47. Two ways to connect to the Internet include connecting by an ISP or directly connecting by means of an Internet Protocol ("IP"). See id. Most large corporations or universities have their own ISP. See id.

20. See Robyn Forman Pollack, Creating the Standards of a Global Community: Regulating Pornography on the Internet—An International Concern, 10 TEMP. INT'L & COMP.

^{13.} See BERNARD ROBIN, ELISSA KEELER & ROBERT MILLER, EDUCATOR'S GUIDE TO THE WEB 1-2 (1997) (noting the Internet has changed from being a tool solely for scientists and researchers to a public information tool which allows millions of people all over the world to communicate).

^{14.} See ED KROL & PAULA FERGUSON, THE WHOLE INTERNET FOR WINDOWS 95 26-30 (1995) (information sent across information protocol networks is broken up into bite-sized pieces called packets and thereafter sent via a transmission control protocol to be recombined at a destination).

user may "encrypt" his or her transmission so the receiver of the message has no capability of knowing who sent it.²¹ Therefore, the structure of the Internet allows persons to transmit any type of information with few repercussions.²² Thus, governments of all Internet using countries are faced with a dilemma: how to allow the free exchange of information while at the same time prevent socially unacceptable information from entering their country via the Internet.²³

B. INTOLERABLE INFORMATION

Although many Internet crimes are possible, this paper focuses on socially intolerable information.²⁴ Governments of each country have differing views as to what they regard as intolerable information.²⁵ For

22. See Steven Levy, The Encryption Wars: Is Privacy Good or Bad?, NEWSWEEK, Apr. 24, 1995, at 55 (noting the FBI believes encryption is a powerful tool for criminals to freely exercise fraud and drug trafficking to the point national security may be threatened).

23. See Ari Staiman, Shielding Internet Users From Undesirable Content: The Advantages of a PICS Based Rating System, 20 FORDHAM INT'L L.J. 866, 889 (1997). The European Union ("EU") (consisting of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Spain, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Sweden, and the United Kingdom) guarantees freedom of expression and each of the countries allow for freedom of expression in their respective constitution. See id. Additionally, the United States provides for protection of one's freedom of expression. Id. at 898. In addition to the United States and the EU recognizing a need for protecting children for Internet pornography Canada and Singapore have launched their own forms of protection; Pollack, supra note 20, at 487. The Canadian Association of Chiefs of Police recommended that the government create a specific Criminal Code offense for the distribution of pornography over computer networks. See id. In Singapore, authorities announced plans to create a "neighborhood police post" on the Internet to monitor and to receive complaints regarding the distribution of pornography. See id.

24. The term "socially intolerable information" differs for each country. For example, in the United States pictures and drawings explicitly depicting men and women in groups of two or more engaged in sexual activities with their genitals displayed was enough to trigger a California criminal obscenity statute. See Miller v. California, 413 U.S. 15, 16 (1973). Compare the situation where an Islamic cleric requested that the United States State Department extradite pop singers Madonna and Michael Jackson to Pakistan because their music violates Islamic law. Madelain Drohan, Nations See Internet as Threat to Security, DALLAS MORNING NEWS, Feb. 11, 1996, at 20A; see Internet Hate Sites Double in 1 Year, CHI. TRIB., Nov. 13, 1997, § 1, at 18 (according to the Simon Wiesenthal Center, hate related web sites have doubled in the past year to over 600). In addition to pornography many nations deem hate information such as instructions on bomb making to be intolerable information. See id.

25. See Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, COM(96)483 at 15 [hereinafter Green Paper] (noting that the

L.J. 467, 480 (1996). A person sending a message may conceal his or her identity by way of an "anonymous remailer." See id. An anonymous remailer is a type of information transmission where a sender sends the message to a service which receives the message, relabels the electronic address and sends the message. See id.

^{21.} See PIKE, supra note 6, at 296 (stating "encryption" constitutes a method of altering a message to make it incomprehensible to any third party intercepting the message).

instance, the United States has separated socially intolerable information into two categories: material that is typically referred to as "adult," termed "obscene"²⁶ and information socially unacceptable, devoid of any useful expression, termed "indecent."²⁷

Currently, the United States and the European Union ("EU") have similar views on intolerable material on the Internet. Both the United States and the EU believe adolescents should not be exposed to either indecent or obscene information.²⁸ Materials likely to affect the mental

member states universally agree sexually explicit material is socially intolerable). Specific member states including Austria, Belgium, Denmark, the Netherlands, and the United Kingdom define and regulate child pornography with specific legislation. *Id.* at 37. Other member states including Luxembourg, Portugal, and Spain define and regulate child pornography by general obscenity rules. *See id.*; see East Asian Censors Want to Net the Internet Autocrats in China, Singapore, Burma, and Other Countries, CHRISTIAN SCI. MONITOR, Nov. 12, 1996, at 19 [hereinafter East Asian Censors] (noting that China finds information published within the Los Angles Times, Washington Post, New York Times, and Wall Street Journal socially intolerable and a threat to national security). Burma prohibits sending or receiving information regarding state security, economy, and national culture. *Id.* at 19; Andrew Brown, *EU Racism Demands Internet Neo-Nazi Censorship*, INDEPENDENT (LONDON), Jan. 30, 1996, at 3 (in addition to sexually explicit material, the display of Nazi symbols and the expression of pro-Nazi sentiments are illegal under German Law).

26. See Miller, 413 U.S. at 17. The Supreme Court in Miller set forth a three prong test to determine whether material can be classified as "obscene." See id.

The three prongs include: (1) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; and (2) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (3) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id.

27. F.C.C. v. Pacifica Foundation, 438 U.S. 726, 727 (1978) (finding a statue was unconstitutional which banned certain words from being spoken during a broadcast). The *Pacifica* court defined the words "obscene" and "indecent." *See id.* The term "obscene" describes words or materials which are not constitutionally protected but neither state governments nor the federal government may prohibit possession of "obscene" materials in the privacy of one's home whereas "indecent" words or materials are non-protectable. *Id.* at 727. *See generally* Stanley v. Georgia, 394 U.S. 557 (1969); *Miller*, 413 U.S. at 15 (noting that the Supreme Court upheld the constitutionality of a California law which banned obscene material as applied to a defendant who mass mailed materials depicting couples having sex with their genitals exposed).

28. See Yaman Akdeniz, Pornography on the Internet (visited Sept. 16, 1997) <http:// www.leeds.ac.uk/law/pgs/yaman/artporn.htm>. Section 1(1) of the 1959 United Kingdom Obscene Publications Act (1959) defines obscene as:

For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. health of adolescents are the most distained by these governments.²⁹ Although most of the other global nations are opposed to the same materials, there are some nations which find less innocuous material unacceptable.³⁰ For example, Malaysia recognizes the Internet includes predominantly Western philosophy-type subject matter which goes against Malaysian society and culture.³¹

C. INTERNET REGULATION EFFORTS

The United States accounts for almost half of all host computers capable of transmitting information over the Internet. Germany is second with nearly 453,000 host computers. The United Kingdom ranks third.³² These countries are attempting to regulate information over the Internet by various methods with varying degrees of effectiveness. The following is a summary of several notable countries and their methods of regulation:

1. United States

On February 8, 1996, the Telecommunications Act³³ was passed into law, including a provision known as the Communications Decency Act

^{29.} See Report on the Commission Communication on Illegal and Harmful Content on the Internet, COM(96)487 [hereinafter Commission Report]. The EU recognizes "harmful content" to mean both content which is allowed but whose distribution is restricted (adults only) and content which may offend certain users. See id.

^{30.} See East Asian Censors, supra note 25, at 19 (noting the Chinese government protects its people from information within some of the United States top news publications (e.g., the Los Angeles Times, Washington Post, New York Times and the Wall Street Journal).

^{31.} See KL Looking Into Ways to Censor Internet, SING. STRAIT TIMES, Sept. 23, 1996, at 23 (noting that although the Malaysian Government recognizes economic benefits of the Internet, it believes that Western culture and values dominate the Internet, and could be a threat to Malaysia's culture, values, and business systems).

^{32.} See Shailagh Murray & Richard L. Husdson, Europe Seeks to Regulate Global Internet, WALL ST. J., Mar. 18, 1996, at A1. See also Lottor, supra note 12 (noting the current global growth rate of host computers is 70% per year and the United States continues to possess between 40% and 60% of all the host computers world wide). The top level domains or countries with the most Internet connections include: Australia, Austria, Belgium, Brazil, Canada, China, Czech, Denmark, Finland, France, Germany, Hong Kong, Hungary, Ireland, Israel, Italy, Korea, Malaysia, Mexico, Netherlands, Norway, New Zealand, Poland, Portugal, Russian Federation, South Africa, Spain, Sweden, Switzerland, United Kingdom, United States. See id.; see also John Quarterman (visited Nov. 15, 1997) http:// www.mids.org/> (depicting additional estimates of Internet connected countries with three letter global domain names).

^{33. 47} U.S.C. §§ 223 (a) - (h) (1996). The purpose of the CDA is to restrict access by minors to "patently offensive depictions of sexual or excretory activities" on an "interactive computer service." See id. The Telecommunications Act proposed to give consumers much wider choice for their cable TV and telephone service providers. See id.

("CDA").³⁴ A day after President William J. Clinton signed the bill enacting the CDA as law, a lawsuit was filed to contest the constitutionality of the law.³⁵ The Supreme Court held the CDA unconstitutional.³⁶ The Court stated the CDA invoked a standard equal to the most stringent community standard triggering what is known as the "lowest common denominator effect."³⁷ Additionally, the CDA had no effect on foreigners who transmitted indecent and pornographic material over the Internet throughout the United States.³⁸ Subsequent to the Supreme Court finding the CDA unconstitutional, President Clinton decided not to promote legislative measures to regulate the Internet.³⁹

2. Germany

The German government has taken a "no toleration" approach to the Internet by forcing ISPs to block web sites displaying pornography or Nazi propaganda.⁴⁰ In 1995, the Bavarian Justice Ministry informed CompuServe Inc. that senior company officials could face prison terms for violation of German anti-pornography laws.⁴¹ In 1996, Deutsche

^{34. 447} U.S.C. §§ 223(a), (d). In § 223 (a), the CDA, defines regulated material as "obscene or indecent" while in § 223 (d) it defines it as material which is "patently offensive as measured by contemporary community standards." *See id.* The United States district court for the Eastern District of Pennsylvania issued a preliminary injunction against CDA enforcement on grounds the terms "patently offensive" and "indecent" are sufficiently vague. American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).

^{35.} See generally ACLU, 929 F. Supp. at 835.

^{36.} See Reno, 117 S. Ct. at 2351. The Supreme Court, in finding the CDA unconstitutional, held alternatives existed to protect children from harmful materials and the CDA was unnecessarily broad. *Id.* at 2346. The broad nature of the CDA would act to suppress material addressed to adults, thus violating first amendment rights. See *id.*

^{37.} See Sean Selin, Governing Cyberspace: The Need for an International Solution, 32 GONZ. L. REV. 365, 382 (1996) (noting that the lowest common denominator effect refers to every Internet user being forced to respect the strictest community standard or be held liable to a law determined by members of this community).

^{38.} See Pollack, supra note 20, at 484 (noting even if the CDA were constitutional the CDA is not internationally recognized legislation and therefore foreign countries are not liable under its provisions).

^{39.} See Jodi Edna & Matt Mossman, Clinton Urges Voluntary Net Limits, PHILA. IN-QUIRER, July 17, 1997 at A2. President Clinton participated in a computer industry ceremony including computer industry representatives, library groups and parents' groups agreeing to support a voluntary rating system. See *id*. Voluntary rating systems operate by filtering software blocking specific ratings at the user's terminal. See *id*. Therefore, rating systems depend on an author appending a rating to the material to be uploaded on the Internet. See *id*.

^{40.} See William Boston, Germany Offers Pioneering Bill to Police the Internet, REUTER BUS. REP., Apr. 18, 1997 (stating the German government's technology minister, Juergen Ruettgers, stating that Germany will not tolerate the availability of neo-Nazi material from any German or overseas web site).

^{41.} See John T. Delacourt, Recent Development: The International Impact of Internet Regulation, 38 HARV. INT'L L. J. 207, 212 (1997). German police provided CompuServe a

1998] INTERNATIONAL INTERNET REGULATION

Telecom, a German on-line server, severed access to a neighboring ISP which was renting space to a Californian neo-Nazi web site.⁴² In the wake of Germany's indictment of a CompuServe official, the German government introduced a bill to police the Internet.⁴³

3. China

The Chinese government is apprehensive of allowing unfettered Internet access.⁴⁴ China envisions its relationship with the Internet as one oriented entirely towards business to serve as a tool to spur China's economic development.⁴⁵ The Chinese government implemented "firewall software"⁴⁶ to shield itself from outside influence. Nevertheless, China continues to reap the economic benefits of Internet communication.⁴⁷

42. See Knoll, supra note 8, at 288 (noting that Deutcshe Telekom cut off access to all computers linked to the ISP, Web Communications, for fear of prosecution under tough German anti-Nazi laws).

43. See German Government Tables Bill, supra note 41 (stating new German Cyberspace legislation (the Information and Communications Services Bill) aims to set standards for child protection by defining which activities require regulation and which can be operated without a license or regulatory intervention).

44. See Chinese Rules Passed For Internet Operation, Telecomworldwire, Feb. 6, 1996, available in WESTLAW, TELCOMWW File (noting under Chinese law the Chinese government requires ISPs to register with the government and users are not given access to the Internet unless government approval is issued).

45. See Delacourt, supra note 41, at 215-17 (noting the Chinese government chooses portions of the Internet for Chinese accessibility and blocks the remainder). The Chinese government vehemently contests expression in the forms of pornography and political dissent. See *id*.

46. See Timothy S. Wu, Cyberspace Sovereignty?—The Internet and the International System, 10 HARV. J. L. & TECH. 647, 652-53 (1997) (explaining firewall software as a comprehensive system of network filtration and control elements which allow regulation of information at the gateway or the portion of the Internet that the service provider links the user to the Internet). With a firewall system installed, a country or corporation may prevent inside users from accessing outside sites or outside sites from accessing inside addresses. See id.

47. See Delacourt, supra note 41, at 215-17. To support economic growth China must conduct business with outside countries which will require China to open at least one line of communication to the outside. See id. However, China's firewall technology does not absolutely preclude an outside line from being used to compromise China's isolated system. See id.

list of the discussion groups that contained potentially objectionable material. See id. CompuServe immediately blocked access to all the discussion groups on the police list, however, CompuServe lacking specific blocking technology was forced to "blanket" block nearly all of its four million subscribers merely to accommodate blockage for its German subscribers. See id; see German Government Tables Bill To Police the Internet, DataQuest (India), June 15, 1997, available in WESTLAW, DATAQUEST File [hereinafter German Government Tables Bill] (noting that Germany is the first Western democracy to indict an official of an online service for content the German government deems illegal).

1006 JOURNAL OF COMPUTER & INFORMATION LAW [Vol. XVI

China's Intra-Net⁴⁸ essentially blocks China from the Internet; however, China foresees widespread Internet access for its people in the near future.⁴⁹ In providing Internet access for its people, China plans to follow Singapore's regulation system which would use proxy servers⁵⁰ to monitor transmissions between China and foreign nations.⁵¹

4. Singapore

In March of 1996, the Singapore government announced comprehensive Internet legislation to protect local values.⁵² The Singapore government's Internet regulation system operates by a twofold combination including prosecuting users or Internet providers distributing disturbing information and censoring information transmissions entering through proxy servers.⁵³ The number of censors in Singapore has increased by 80% in a ten year period from 9% in 1983 to 16% in 1993.⁵⁴ The workload per censor has increased five fold from 5,500 pieces per censor in 1978 to more than 25,000 pieces per censor in 1993.⁵⁵

48. See Information Technology: China Opens Up—At Last, 1997 Review of Bus. and Tech., June 1, 1997 (noting the Chinese government term their isolated system as the China Intranet or ChinaNet which serves more than 20 cities in China).

49. See id. (noting China planned to open an Internet gateway link to the rest of the world in 1997 and a number of ISPs are bidding on the service).

50. See ROBIN ET AL., supra note 13, at 165-166 (defining a proxy server as a computer that intercepts Internet traffic and has the ability to keep users from accessing outside web pages); Internet "Filters" Come On Line in Singapore, Agence France-Presse, Sept. 15, 1996, available in WESTLAW, ALLNEWSPLUS File (noting the more than 100,000 Singapore Internet subscribers direct their computer software to interface with the proxy servers before gaining Internet contact and the proxy servers compare the user's request with a list of banned sites and thereafter deny access if a match is made).

51. See Rajiv Chandra, Beiging Turns To Singapore For Tips On Internet Censorship, Inter Press Service, Aug. 7, 1996, available in WESTLAW, ALLNEWSPLUS File (stating China plans to establish a censored international link by first studying Singapore's Internet connections).

52. See Knoll, supra note 8, at 292-94. To support Singapore's regulation of the Internet, the government enacted laws to hold both Internet users and online providers responsible for keeping pornographic and politically objectionable material off the Internet. See id. Furthermore, the Singapore Broadcasting Authority plans to officially police the Internet, and also register any political or religious user groups. See id.

53. See Censorship and The Internet: A Singapore Perspective, Communications of the Association for Computing Machinery, June 1, 1996, available in WESTLAW, ALLNEWSPLUS File [hereinafter Censorship and The Internet] (noting Singapore's method of censorship includes: first, materials going into the home are more heavily censored than those going into the corporate world; second, materials for the young are more heavily censored than those for adults; and third, materials for public consumption are more heavily censored than those for private consumption).

54. See id.

55. See id.

D. REGULATION TYPES

No country's method of regulating the Internet is globally effective. Many proposals for global regulation of the Internet are available and this Comment addresses the prevailing theories.

1. Rating Systems & Screening Software

The Platform for Internet Content Selection ("PICS") endeavors to rate on-line material in nine categories including sex, violence, and profanity on a scale of one to four.⁵⁶ Through screening software, a user can pre-select ratings. The screening software will screen out subject matter having the selected ratings.

Screening software usually takes one of two approaches: either the software blocks those sites which the user identified as undesirable, leaving the remainder accessible, or the software permits access to only those sites which the user identified as desirable, blocking all other sites.⁵⁷ PICS envisions a group of third party individuals periodically reviewing

Id.

57. See Software to Block Internet Access Made Available, Japan Computer Industry Scan, Sept. 22, 1997, available in WESTLAW, JPCIND File (filtering software checks the contents of sites when users attempt access and if the contents are rated at a level ruled out in advance by parents or teachers the software makes the sites inaccessible); Staiman, supra note 23, at 887. Screening software typically operates by using one of three types of blocking techniques, which include: whitelisting, blacklisting and blocking by a word and character search. See id. Whitelisting is a blocking method wherein a user can only access Internet addresses which are pre-selected and programmed into the screening software. See id. Blacklisting is a blocking method wherein undesirable Internet sites are programmed into the screening software to be nonaccessible. See id. The third method of blocking invokes a word and character search which screening software reads and if the preprogrammed character or word is identified by the software then access to that site is denied. See id.

^{56.} See Delacourt, supra note 41, at 225-27 (noting that the PICS rating system operates by relying on each user to rate the material he or she downloads to the Internet thereby providing the party viewing this material an option to view depending on the rating). See also ROBIN ET AL., supra note 13, at 174-175. The Recreational Software Advisory Council on the Internet ratings ("RSAC") is an organization that has developed a rating scheme which compliments the PICS rating system. See id. The ratings are as follows:

LANGUAGE: 0 = inoffensive slang, no profanity; 1 = Mild expletives or mild terms for bodily functions; 2 = Moderate expletives, nonsexual anatomical references; 3 = Vulgar language, obscene gestures; use of epithets; 4 = Extreme crude language, explicit sexual references. NUDITY: 0 = None; 1 = Revealing attire; 2 = Partial nudity; 3 = Frontal Nudity, 4 = Provocative frontal nudity. SEX: 0 = No sexual activity portrayed; 1 = Passionate kissing and touching; 2 = Clothed sexual touching; 3 = Nonexplicit sexual activity; 4 = Explicit sexual activity. VIOLENCE: 0 = No aggressive, natural, or accidental violence; 1 = Creatures injured of killed or damage to realistic objects; 2 = Humans or creatures injured or killed; 3 = Killing with blood and gore; 4 = Wanton and gratuitous violence.

ratings to ensure good faith reporting.58

2. Internet Service Providers Acting as Censors

Network providers such as CompuServe could monitor their subscribers network functioning as a gatekeeper.⁵⁹ The Internet does not readily conform to traditional notions of jurisdiction and a state's ability to impose sanctions on violators of the law is dependent on the need for physical control.⁶⁰ However, the burden of holding ISPs liable for content distributed to users is not a realistic solution due to each country's differing standards of intolerable information. In addition, if the ISPs were held accountable for information content, the efforts required to censor the immense amount of material traveling across the Internet would overwhelm ISPs.

3. Technology

(a) Filtering. Filters search for, and block out, intolerable information by looking for key words or phrases. A technical working group including members from the National Computer Board, the National Science and Technology Board and the National University of Singapore is conducting trials to see if filters can be used in censorship for use in Singapore.⁶¹ The current state of filtering software provides an unrealistic solution to Internet regulation due to the vast amount of information traveling across the Internet and the time required to properly filter all information.

(b) Patrolling the Internet. The Internet lends itself to traffic analysis. Traffic analysis may not disclose the information content, however, the source and destination can suggest certain interests.⁶² Once again,

^{58.} See Amelia Hill, Trying to Mend Gaps in the Net, GLASGOW HERALD, Oct. 1, 1997, at 13. In May 1997, Peter Dawe created the Safety Net Foundation which launched the Internet Watch Foundation ("IWF"). See id. The IWF requests service providers to adopt the PICS standard and encourages the on-line community to contact the IWF if obscene information is detected or if information is not rated correctly. See id.

^{59.} See Wu, supra note 46, at 651 n. 15 (noting the gateway describes the point of entry controlled by an Internet service provider or gatekeeper, through which all information must pass if this information is to enter or leave the network).

^{60.} See Knoll, supra note 8, at 299-301. If a provider implemented the proper technology they could alter their gateways to comply with each separate country's laws, provided that those laws are not vague or unworkable. See *id*. Essentially, the global Internet would be run by private corporation. See *id*.

^{61.} See Censorship and the Internet, supra note 53. Negative aspects of filtering include slower access time to the Internet. See *id*. Increased time on the Internet adds to the on-line costs. See *id*. Filters can also filter out useful materials along with the undesirable material. See *id*.

^{62.} See id. For example, if traffic to a particular overseas site is known to contain undesirable material then this site may be more closely monitored. See id. The sheer

1998] INTERNATIONAL INTERNET REGULATION

the vast structure of the Internet renders this solution untenable.

(c) Creation of a Separate Server.⁶³ It has been stipulated by the Singapore government that for an approximate cost of \$70,000 US dollars a year, a separate server to censor Usenet⁶⁴ groups may be implemented on the Internet.⁶⁵ Some users will have access to materials that others do not.⁶⁶ This solution could be effective, however, the benefit of having worldwide communication is thwarted when a country alienates or limits itself from access to other countries.

4. Creation of International Laws

Currently, international law governing the Internet does not exist. However, several individual countries impose legislation in an attempt to decrease intolerable information. The problems associated with each country exercising its own Internet regulation legislation is obvious.⁶⁷ Other forms of technology that distribute information have been successfully governed by international law. Satellites, telephone and computer networks link almost all parts of the earth. These links create new opportunities for people to communicate and act around the world. While current international law covers satellite and telephone networks, there are no laws covering the specific problems of the Internet. Several preliminary steps have been taken in the direction of creating an international convention. A number of Internet-related issues were raised at various meetings in preparation for draft resolutions.⁶⁸

For instance, the Computer Misuse Act⁶⁹ includes specific provisions

64. Id. at 159. USENET refers to a network of computers including all sites that participate in the exchange of network news. See id.

65. See Censorship and the Internet, supra note 53.

66. See id. This will prevent all but the most determined from accessing those censored groups. See id. Drawbacks include the high cost of managing a system to regulate the global Internet. See id. Also, Usenet may be accessed through other providers, therefore, a user may take a detour around such attempted censorship. See id.

67. See Selin, supra note 37, at 383-87. A problem of trilateral jurisdiction arises, rather than a simple application of a nation's jurisdiction over a wrongdoer. See id. Trilateral jurisdiction questions arise when a person at a computer in a first country (first jurisdiction) manipulates a program or accesses a computer in another country (second jurisdiction) and violates law in a third country by displaying or making accessible intolerable information to the third country (third jurisdiction). See id.

68. See Wu, supra note 46, at 660. The Council of Ministers endorsed a French proposal for a "Charter for International Cooperation on the Internet." See id.

69. See Computer Misuse Act, 1990, ch. 18, § 1 (Eng.). Pertinent portions of the Act include:

amount of information and activity on the Internet makes this method highly improbable for widespread regulation. See id.

^{63.} See DOUGLAS E. COMER, THE INTERNET BOOK 124 (1995). A client uses the Internet to contact a server, therefore a server is any entity that provides service to the Internet. See id.

pertaining to jurisdiction, including citizenship and extradition. This act applies to people who commit computer misuse in a foreign jurisdiction if the particular misuse is recognized in the foreign jurisdiction, as well as in the jurisdiction seeking criminal charges.⁷⁰

Foreseeable problems arise in enforcing international laws enacted to regulate the Internet since countries hold vastly different political and social values. Freedom of speech is not a universally held belief. Problems inevitably arise when a country such as Germany wishes to prosecute a United States citizen for placing pro-Nazi propaganda on the Internet.⁷¹ The United States is hesitant to support extradition in view of the United States citizens First Amendment rights, whereas the German government desires to prosecute the United States citizen under German law.

III. ANALYSIS

The Internet represents a network of networks and not a single system as the term may connote. Governments attempted to regulate the Internet with little understanding of the structure of the Internet.⁷² This Comment analyzes the Internet's unique structure, identifies methods of regulation and advocates a flexible structure to accommodate a range of regulatory systems. Moreover, this Comment proposes a unique solution to international Internet regulation defined as the "Multinational Approach." The Multinational Approach is then applied to a common paradigm and thereafter two main government regulation methods are critiqued in view of the Multinational Approach.

⁽¹⁾ A person is guilty of an offense if —

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; . . . Id.

^{70.} See Selin, supra note 37, at 387.

^{71.} See Knoll, supra note 8, at 288-89. In late January 1996, Deutsche Telekom cut off access to all computers linked to Web Communications, another on-line server for fear of prosecution under German anti-Nazi law since Web Communications rents web space to Ernst Zundel, a German neo-Nazi expatriate living in California.

^{72.} Renov. American Civil Liberties Union, 117 S. Ct. 2329, 2338 n.24 (1997). Senator Leahy states:

It really struck me in your opening statement when you mentioned, Mr. Chairman, that it is the first ever hearing, and you are absolutely right. And yet we had a major debate on the floor, passed legislation overwhelmingly on a subject involving the Internet, legislation that could dramatically change—some would say even wreak havoc—on the Internet. The Senate went in willy-nilly, passed legislation, and never once had a hearing, never once had a discussion other than a hour or so on the floor.

INTERNATIONAL INTERNET REGULATION

A. INTERNATIONAL REGULATION IS WARRANTED

The Internet allows people of a nation to freely and expediently interface with people of any other Internet connected nation. When countries disagree with each other's laws, they tend to isolate themselves to sustain control. Therefore, an international regulation effort is critical to uphold the international scope of the Internet. The dilemma which is shared by Internet-connected countries is that the Internet promotes a society's learning opportunities and fosters economic growth while providing a safe haven for anonymous porn distributors.⁷³

Most global regulation theories are flawed for at least one reason in that global regulation requires all countries to abide by the regulation set by the country with the most stringent regulatory policy.⁷⁴ Under such a policy, many societies would be banned from freely exchanging messages, ideas and information that would be otherwise valuable to the progress of society.⁷⁵

Global regulation has not been exclusively embraced because governments disagree on Internet regulation. Countries interested in protecting societal values have to approach Internet regulation more aggressively than countries which support free expression. A harsh but effective solution for societal value protective countries is to either sever themselves from the Internet or limit their Internet connections to only a few terminals. This drastic measure depicts the lack of communication between nations over the issue of Internet regulation. Moreover, nations comfortable with an effective international solution would not take such drastic measures, thus, an international solution is a sensible one.

^{73.} See Commission Report, supra note 29, at B1. The committee states: Permitting total freedom of expression, the Internet has resurrected the utopian dream (inherited from the libertarian ideas of the US researchers who conceived it) of a harmonious global human community in which every member develops his knowledge with the help of others. Another problem arises from the use made of the Internet by pornographers, pedophiles, holocaust deniers, sects, and other purveyors of highly objectionable messages. However, the particular nature of the Internet is such that censorship is virtually impossible. If a message is blocked from passing through one channel, it can get through by another.

Id.

^{74.} See generally Reno, 117 S. Ct. at 2352 (noting the proposed Communications Decency Act ("CDA") would protect children from undesirable content, however, it may would also prevent adults from accessing legal content); Douglas Hayward, Regulating the Internet Is an International Job, TECHWIRE, June 27, 1997. Felipe Rodriquez, a managing director of a Dutch Internet service provider stated, "The CDA intended to implement measures that would change the Internet we know and love into a kindergarten, of course, we need to address the issues of illegal and harmful content, but one should not overreact and try to fight the Internet, its users and its industry." See id.

^{75.} See COMER, supra note 63, at 4 (noting the most significant aspect of the Internet is its impact on society since the Internet has expanded into governments, businesses, schools, and homes worldwide).

B. A FLEXIBLE REGULATORY SYSTEM

An international system will not operate if a single regulatory solution is rigidly enforced. Each nation has differing tolerances to egregious subject matter and a successful system must accommodate a range of control efforts. For example, the Singaporean government employs aggressive measures to 'prevent' socially unacceptable material.⁷⁶ In contrast, the EU has proposed screening software and PICS, a less aggressive measure, to 'protect' EU citizens of unacceptable material.⁷⁷

In attempting to regulate the Internet, countries generally use one of two approaches. The first approach includes regulatory measures controlled by the government or 'government censorship.'⁷⁸ The second approach includes regulation by the user or 'self-regulation' by ISPs.⁷⁹ In an ideal Internet environment, government regulation strives for no tolerance of socially disturbing information at any juncture of the global network.⁸⁰ In contrast, self-regulation acknowledges the presence of indecent material on the Internet. However, due to the structure of the

78. See Vijay Joshi, Singapore Launches Effort to Police the Internet: Pornography, Criticism of Government, Discussions of Race and Religion Have Officials Worried, FRESNO BEE, Aug. 15, 1996, at C2. An example of government regulation includes the Singapore government approach to regulation which employs proxy servers or government censors to conduct surveillance on incoming and outgoing Internet transmissions. See id.

79. See Hill, supra note 58, at 13. An example of self-regulation includes the Danish government's implementation of the PICS rating system and filtering software. See id.

80. See Chinese Rules Passed For Internet Operation, Telecomworldwire, Feb. 6, 1996, available in WESTLAW, TELCOMWW File. A news service broadcasting Chinese Internet news stated:

The Chinese government has finally published its long-awaited rules which seek to regulate all access links to the Internet, forcing firms to liquidate and register their presence as authorized Internet providers. The government is clamping down heavily on pornography and so-called political content' and while the directive gives government approval to the Internet, Chinese users will not be given free-reign over the diverse computer network. The state will control international links to the Internet and permits must be obtained from a plethora of ministries and official bodies. Additionally, one of the regulations effectively screens' the users of Internet services to ensure that the more undesirable elements do not get access. Unspecified legal sanctions are mentioned for law breakers.

Id.

See also New Internet Regulations Set For Germany, Internet Business News, May 1, 1996, available in WESTLAW, INTBN File. Juergen Ruettgers a German research and technology minister stated, "the [German] government could not tolerate the Internet distribution of neo-Nazi propaganda, child porn or other illegal materials over the Internet." See id.

^{76.} See Staiman, supra note 23, at 898. The government of Singapore empowers an agency, the Singapore Broadcasting Authority ("SBA"), to protect children against intolerable material on the Internet by requiring ISPs to obtain a license from the SBA and thereafter block sites on the Internet as directed by the government.

^{77.} See Green Paper, supra note 25, at 2 (the EU stating an effective regulation system consists of a neutral labeling system as proposed by PICS and a filtering system attached to each terminal allowing parents to avoid ranked materials corresponding to indecency).

Internet and the protection of freedom of expression, self-regulating countries confront this material at its terminal destination.⁸¹ Whether a nation's government chooses government censorship or self-regulation may reflect the government's relationship with its people.⁸²

Regardless of the structure of the Internet, a government has some control over its people and the introduction of a new technology into a nation should not upset the delicate balance between a nation and its people.⁸³ The various national governments⁸⁴ comprising the Internet typically respect each others control over their people.⁸⁵ However, the Internet metropolises have yet to seriously consider other nations regu-

The Antelope, 23 U.S. (10 Wheat.) 66 (1825).

^{81.} See Commission Report, supra note 29, § A. Two imperative elements regarding freedom of expression are raised by the commission which include: first, no person should be made to suffer for his opinions, and the free communication of ideas and opinions is a fundamental right in all democratic societies. See id. Second, freedom of expression on the Internet fosters encouragement to the development of communications to further cultural, economic and social spheres between nations. See id.; see Peter Leonard & Peter Waters, Censoring the Net in Australia: Brave New World or 1984 Revisited?, in 4 THE COMPUTER LAW ASSOCIATION COMPUTER LAW COMPANION 195, 207 (C. Ian Kyer et al. eds., 1996) (noting the Internet is essentially unregulatable except for screening rated material at its end destination).

^{82.} See Deborah Cole, Dertouzos Accepts Internet Smut Control, (visited Sept. 26, 1997) <http://biz.yahoo.com/finance/97/09/29/y0026_y00_1.html>. Dertouzos, a United States Internet expert and Massachusetts Institute of Technology professor commenting on whether Germany's efforts to aggressively fight pornography and neo-Nazi propaganda is an attack on free expression stated, "[m]y belief is that countries should preserve their cultures. We have trade and criminal law cross-nationally. Ministers should get together and create cross-national laws on the Internet." *Id*.

^{83.} See Jonathan Manthorpe, Asia Targets Flow of Information on the Internet: Singapore is at the Forefront of Asia's Movement to Counter Western Influence in the Region, VANCOUVER SUN, Mar. 18, 1996 (hundreds of Chinese citizens were killed in 1989 at Tiananmen Square when government protesters fought with police after an anti-government writing by Wei Jingsheng was circulated); see Chandra, supra note 51 (China's Information Minister, George Yeo, believes that an unregulated Internet provides access to prodemocracy activists living both in and outside of China which cause social discontent and political instability); Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2346 (1997) (the Supreme Court noting a commonality between constitutional anti-pornography legislature for broadcasting and regulation of the Internet stated that, "It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials").

^{84.} See Lottor, supra note 12 (to date 176 countries are connected to the Internet and experts foresee the overall exponential growth rate of Internet connections to continue).

^{85.} Analysis of international law is beyond the scope of this article, however, Untied States Chief Justice Marshall in deciding whether to apply United States law on foreign nations stated:

No principle of general law is more universally acknowledged, than the perfect equality of nations. Russia and Geneva have equal rights. It results from this equality, that no one can rightfully impose a rule on another. Each legislates for itself, but its legislation can operate on itself alone.

lation efforts.86

C. The United States and the European Union Alienate Other Countries

The United States and the EU governments foresee a practical solution to Internet regulation in PICS and screening software. However, in so doing they have sought no international consensus. Other counties will probably not follow the United States and EU's effort because this method does not offer an exclusive means for government control. The EU has formed a commission specifically to address Internet regulation.⁸⁷ The EU appointed a commission to draft a series of questions which address the proliferation of indecent material on the Internet.⁸⁸ The document is called "The Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services" (hereinafter Green Paper).⁸⁹ The main focus of the Green Paper is to implement a

87. See Commission Report, supra note 29, § 1 (noting European Telecommunications Ministers and Culture Ministers staged an informal meeting to urgently address the issue of illegal and harmful content on the Internet).

88. See id. The Telecommunications Council met in Bologna on Apr. 24-25, 1996 to set up a working party to address ethical problems raised by the Internet. See id.

89. See Green Paper, supra note 25, chs. 2-3. The following questions were drafted by the committee:

(1) Taking account of what is technically feasible and economically reasonable, what should be the liability of different operators in the content communication chain, from the content creator to the final user? What types of liability - penal, civil, editorial - should come into play and under what conditions should liability be limited? (2) How should the test of proportionality of any restrictive measures be applied? Inter alia, should any arbitration or conciliation mechanisms at European Union level be envisaged? If so, what sort of mechanisms? (3) How do we determine the right balance between protection of privacy (including allowing users to maintain anonymity on the networks) and the need to enforce liability for illegal behavior? (4) Should one give priority to a regulatory or a self-regulatory approach (possibly backed up by legislation in the latter case) as regards parental control systems? What measures would be required, inter alia at European Union level? (5) In what cases should systematic supply of parental control systems be envisaged? If so, in what form and to which operators should it apply? What are the essential functions that such systems should provide? (6) How can decentralization of content rating be implemented, catering for the need to respect individual, local and national sensitivities, where audiovisual and information services are transnational? (7) What elements of standardization would allow content ratings to be developed in a coherent way in Europe, in particular in the case of digital services (standardization of types of information to be supplied, of encoding and decoding of such information, etc.)? (8) In what ways should administrative coop-

^{86.} See generally Green Paper, supra note 25. The EU raises the issue of whether international cooperation is a high priority when drafting the Green Paper, however, the EU proposes a rating system approach to regulation before international considerations are addressed. See *id*; the United States constructed the CDA having foreign implications without international consensus. 47 U.S.C. § 223 (a) (1996) (the statute attempts to include foreign sources of indecent and obscene materials by stating, "(a) Whoever in interstate or 'foreign' communications . . .").

1998] INTERNATIONAL INTERNET REGULATION

unique system of self-censorship.⁹⁰ The Green Paper explicitly cites PICS as the method of EU Internet regulation.⁹¹ PICS has the support of both the EU and the United States.⁹²

The Green Paper addresses the current structure of the Internet and its lack of regulation.⁹³ The Green Paper states a unitary solution must be found in order to make regulation effective.⁹⁴ PICS is an attractive solution because governments can remain essentially free of burden and current levels of free expression are not decreased.⁹⁵ However, this type of regulation is not a solution in the eyes of many nations.⁹⁶

Id.

90. See id. See questions 5 and 9. See id. Essentially the Committee envisions the PICS ranking system coupled with a filtering system to provide a flexible system that may be applied internationally. See id.

91. See Staiman, supra note 23, at 883-84. The Platform for Internet Content Selection ("PICS") was developed by the World Wide Web Consortium ("WC3") and consists of technical specifications that provide Internet standards for rating formats. See id. The author makes an effective description of PICS by stating, "PICS is analogous to specifying the place on a package that a label should appear and the size of the label, without specifying what the label should say." See id.

92. See Jodi Enda, Clinton Urges Voluntary Net Limits, PHILA. INQUIRER, July 17, 1997 (noting that President Clinton publicly supports voluntary rating systems and filters allowing parents to tailor their home computer systems to protect their children from the higher rated materials).

93. See Green Paper, supra note 25, ch. 2 (noting the Internet represents a new model of interactive communication and that each new user becomes a potential supplier of material, therefore, this unique model defies any simple analogy with existing media and traditional forms of telecommunications).

94. See id., ch. 3, § 4. Question 9 expresses a twofold concern being what regulation solution will work internationally and should the international regulation solution be conducted first or subsequent to exercising an EU regulation solution. See id.

95. See Staiman, supra note 23, at 904. The author makes the point that PICS is the most effective "preventative" solution because it prevents retrieval of indecent materials while upholding the "four freedoms" recognized by the EU (free movement of goods, persons, services and capital). See id.

96. See Delacourt, supra note 41, at 227 (for a rating system to be effective every user must rate his or her material otherwise rating systems will be ineffective and moreover censoring countries will not trust citizen controlled regulation); Lawrence W. Fisher, Internet rating system proposed: Cyberspace: Microsoft, Netscape and Progressive Networks Announce the Venture Just as the Senate Works on an Online Obscenity Bill, ORANGE COUNTY REG., June 15, 1995 (the continuing presence of unrated material is a weakness of a United States based rating system, especially in light of the fact that much of the material considered objectionable in the United States originates from foreign sites).

1015

eration be implemented in the European Union? How and in what institutional framework should it be formalized? (9) What should the priorities be at the European level and at international level? In particular, should one give priority to developing solutions at European Union level and then promoting them at international level or should this be done in parallel? What are the most appropriate international fora for international cooperation (G7, OECD, ITU, WTO, UN or bilateral relations)? How should this international cooperation be formalized?

D. A MULTINATIONAL APPROACH TO INTERNET REGULATION

One rigid unitary solution to international Internet regulation is impossible.⁹⁷ However, each country's individual effort acknowledged and accepted into a flexible structure is a solution.⁹⁸ A flexible regulatory structure will provide at least two benefits. First, each participating country will benefit by having the ability to exercise its own form of regulation. Second, the Internet will likely benefit by providing an international forum which may be more likely to slow the spread of intolerable information.⁹⁹ The flexible system relies on each governments' ability to control ISPs.¹⁰⁰ ISPs undeniably provide a focal point of web site controllability since web sites could not be accessed if all ISPs decided to disconnect service.¹⁰¹ Furthermore, United States experts believe even the slightest government intervention will protect the Internet from an

^{97.} See The Cutting Edge; Testing the Boundaries; Countries Face Cyber Control in Their Own Ways, L.A. TIMES, June 30, 1997, at D1 (a regulation solution among nations is impossible since nations disagree on regulation theories and in addition, the borderless nature of the Internet poses regulation difficulties).

^{98.} See Katherine Sainty & Julia Horsley, Current Information Technology Issues in The Pacific Rim, 4 THE COMPUTER LAW ASSOCIATION COMPUTER LAW COMPANION 253, 276 (C. Ian Kyer et al. eds., 1996). Strictly controlled access regimes as exercised by the Chinese and Singaporean governments are effective methods of censorship, however unappealing to Western society. See id. On the other end of the spectrum is self-regulation and anything in between is likely to cause uncertainty and difficulties in implementation. See id.

^{99.} See Censorship and the Internet, supra note 53. Generally a country finds it difficult to block international sites known to contain intolerable information since users will simply bypass local service providers and access the material from overseas providers. See id.

^{100.} In implementing a flexible regulatory system which facilitates the least regulatory scheme (self-regulation) and the strictest regulatory scheme (government censorship), the Internet service providers must cooperate with a body which aims to decrease intolerable information. See id. See David Kerr, Who is Going to Carry the Can? Assigning Responsibility For Internet Content; Industry Trend or Event, COMPUTER WEEKLY, May 22, 1997 (noting the United Kingdom police and representatives of ISPs have made an agreement in which the ISPs will remove intolerable information after being notified by web users calling a complaint line (the Internet Watch Foundation) in exchange for the police not filling a court action against the ISPs). See Singapore - Government Clamps Down on Internet and Supports Its Future, Telenews Asia, Mar. 21, 1996, available in WESTLAW, TNASIA File (the Singapore government mandates ISPs to register for a license and remove content considered to be in breach of Singapore laws). However, ISPs may not uniformly cooperate with the body unless it is forced to do so. See Police Give Icy Reception to Demon Net Monitoring Plan Refuses to Bar Access to Many Internet Newsgroups That Contain Illegal Material, Computing, Sept. 5, 1996, available in WESTLAW, COMPUTING File (Demon, a United Kingdom ISP, refused to remove newsgroups that contained what police say was illegal information, stating that they are not legally accountable).

^{101.} See COMER, supra note 63, at 125 (noting when a service provider's computers loses power then all servers running on the computer are lost and clients using that server will receive an error message).

unforeseeable disaster.¹⁰²

The Multinational Approach suggests each country's regulation be evaluated and useful portions considered. An evaluation of several countries regulation efforts serve to identify the corresponding government's attitude toward intolerable information. For example, Germany found a temporary solution by forcing CompuServe to block particular sites or face fines and imprisonment.¹⁰³ The result was CompuServe acted quickly to block the sites.¹⁰⁴ The United States and the EU foresee PICS providing a universal approach to regulation.¹⁰⁵ Since PICS is currently being tested, uniform enforcement measures have not been implemented.¹⁰⁶ Singapore and China exercised direct governmental control over the Internet by implementing proxy servers and firewall technology, respectively, to censor transmissions within these countries.¹⁰⁷ Should a

103. See Mitchell Martin, Germany Forces CompuServe to Censor Sex on the Internet, INT'L HERALD TRIB., Dec. 29, 1995 (noting the German government made CompuServe officials aware of an anti-obscenity law which held ISP officials criminally liable therefore CompuServe banned 200 sites worldwide having "alt.sex" in their titles).

104. See id. CompuServe did not have the capability to block "alt.sex" sites exclusively for German Internet customers therefore CompuServe shut down "alt.sex" worldwide. See id.

105. See Green Paper, supra note 25 (noting that the EU supports PICS); Enda, supra note 92 (noting President Clinton supports a PICS type labeling system).

106. See Steven Lynch, The Rating Game Online: A High-Tech Coalition Has Decided How to Clean Up the Internet—By Having Sites Rate Themselves, ORANGE COUNTY REG., Mar. 31, 1996, at K9 (noting select site administrators have rated themselves and SafeSurf, a Van Nuys Internet software company, had each worker review the self-ratings at a rate of 300 to 500 sites a day); Charles Arthur, Internet Could Get Cinema-Style X-Ratings in Purge on Porn, INDEPENDENT (LONDON), July 1, 1997, at 5 (stating in the United Kingdom there are hundred of thousands of web sites but only 1,419 have ratings and worldwide only 3,500 sites are rated).

107. See Peng Hwa Ang & Berlinda Nadarajan, Censorship and the Internet: A Singaporean Perspective, Communications of the Association for Computing Machinery, June 1, 1997, available in WESTLAW, ALLNEWSPLUS File (notably China and Singapore agree that government censorship in cyberspace provides protection of its country and people).

^{102.} See Internet: Internet Stumbles Towards Domain Name Consensus, Network Week, Aug. 15, 1997, available in WESTLAW, NETWORKWK File. Internet pioneers, Robert Kahn and Vint Cerf, instrumental in the creation of Transmission Control Protocol ("TCP") and Internet Protocol ("IP"), opine that the best way to keep the government out of the dayto-day running of the Internet is to find a way to keep them in. See id.; see Dina Elboghdady & Dena Bunis, Regulation of the Internet; Legislation: Foreseeing an Economic Explosion, The White House Wants to Keep the Internet Unfettered, ORANGE COUNTY REG., Jun. 28, 1997. Another source of concern is the inability of the government to regulate or control copyright and trademark infringement which would be harmful to the United States economy if left in the hands of the public to control. See id. Lawrence Lessig, a law professor and Cyberspace analyst at the University of Chicago states, "The view that government should have nothing to do with it is extreme. We don't take that view in real space why should we take that view in Cyberspace?" Id.

country joining the international committee choose the PICS regulation or should they look to Singapore's approach?

A regulation system that could accommodate a range of regulatory interests provides a flexible framework to launch global acceptance of any regulatory system. The framework allowing varying degrees of regulation without alienating a nation should further consist of a governmental agency working in concert with ISPs.¹⁰⁸ The ISP would not be held responsible to censor, rather, the ISP would merely block sites at a government's request.¹⁰⁹ Nations such as the United States and the EU favoring self-regulation could exist with minimal or 'transparent' government intervention.¹¹⁰ Furthermore, the Multinational Approach would avoid the problems inherent in applying overly broad legislation to directly control users.¹¹¹ The ISPs stand the risk of liability if put on no-

109. See Giorgio Bovenzi, Liabilities of System Operators on the Internet, 11 BERKELEY TECH. L.J. 93, 136 (1996). In order to foster the optimum freedom of expression on computer networks, ISP liability should apply only when the ISP knows that an obscene, illegal or defamatory message is posted on the system, or when the ISP does not remove such a message once it has been made aware of its existence. *Id.* Religious Tech. Center v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1372 (N.D. Ca. 1995). The court stated that a rule holding ISPs liable for censoring billions of bits of information flowing through the Internet does not make sense and furthermore, is practically impossible. *See id.*

110. See Green Paper, supra note 25, ch. 2. The EU proposes the PICS rating system, however, the EU unlike the United States does not expressly state whether the government intends to intervene to ensure accuracy and usage of the ratings. See id. Clinton Administration Outlines its Electronic Commerce Policy, 14 No. 3 COMP. L. STRATEGIST 1, (1997). Minimal government intervention aligns with the second principle of President Clinton's five guiding principles to foster the Internet. Id. at 1. The five principles include:

(1) The private sector should be at the forefront of any economic expansion over the Internet, (2) Governments should avoid imposing undue restrictions on electronic commerce, (3) Governmental intervention should be limited to ensuring competition, protecting intellectual property and privacy, preventing fraud, fostering market transparency, supporting commercial transactions and facilitating dispute resolution, (4) The Internet 's unique structure is decentralization and bottom-up leadership, and (5) Global commerce shall be facilitated.

Id.

111. See Selin, supra note 37, at 373. Problems with legislative regulation are twofold, first determination of jurisdiction is difficult due to the Internet's unique structure and second, the legislation may violate a user's right of free expression. See *id.*; Tim Hardy, U.K. Internet Services Seek Legal Change, NATIONAL L.J., Aug. 25, 1997. Nations find it

^{108.} See Singapore Promoting Use of Internet, Xinhua English Newswire, Oct. 7, 1996, available in WESTLAW, ALLNEWSPLUS File (noting the Singaporean government placed a governmental agency, termed the Singaporean Broadcast Authority ("SBA"), in charge of regulating and promoting the Internet). Compare the United States government having the Federal Communication Commission ("FCC") regulate broadcast transmissions. In *Pacifica*, the United States Supreme Court upheld a declaratory order of the FCC, holding a broadcast including monologue referring to excretory or sexual activities or organs to be in violation of federal statute and therefore precluded by the government. FCC v. Pacifica, 438 U.S. 726, 730 (1978).

tice by the government to remove intolerable information and they fail to act.¹¹² The increased cost of requiring ISPs to cooperate with governmental agencies is likely to be less than the cost of implementing PICS and screening software to the millions of computers linked to the Internet. Moreover, ISPs are profit motivated entities that can distribute their costs to the consumer.¹¹³

E. The Multinational Approach Applied to Self-Regulated and Government Censored Nations

Nations which regulate the Internet themselves, such as the United States, would readily conform to the Multinational Approach. As an example, suppose an adolescent, within the borders of the United States, attempts to download indecent images from a web site. The adolescent is unable to do so due to PICS and screening software which block this material.¹¹⁴

In contrast, if a child in Singapore attempts to contact a United States web site, which supposedly exhibits pornographic qualities, the government's proxy server intercepts the images and identifies the United States web site responsible for the socially unacceptable material.¹¹⁵ Singapore contacts the corresponding ISP and has the web site blocked.¹¹⁶ Shortly thereafter, the ISP distributes an international

113. See Tom Nolle, Your ISP Survival Guide, Internetwork, Feb. 1, 1997, available in WESTLAW, INTERNETW File (noting the once profitable ISP business is declining and in order for ISPs to survive they must control the entire connection between a company and its main clients); see Several USA Based Internet Service Providers Are Attempting To Build Global One-Stop-Shop Internet Services, Network World, Aug. 26, 1996, available in WESTLAW, NTWKWLD File (noting several United States based ISPs attempt to provide enhanced Internet service which would avoid the high cost of overseas ISPs and increase the quality of service).

114. See Hill, supra note 58, at 13 (PICS prevents unexpected and unwanted exposure of obscene images).

115. See Internet "Filters" Come On Line In Singapore, supra note 50 (noting that Cyberway, a Singapore ISP, has a system in place to check a user's request to enter an Internet site against a list of 100 banned sites before granting access).

116. Not unlike United States control over published written material, the Singapore government would remove the subversive material from Singaporean access. *See generally*

1019

difficult enough for aggrieved plaintiffs or police authorities to pursue defendants publishing material, however, with the imposition of liability attaching to the ISP, nations have been able to decrease unsuitable material on the Internet. *See id.*

^{112.} See William Boston, Germany Offers Pioneering Bill to Police the Internet, REUTER BUS. REP., Apr. 18, 1997 (depicting the German government's intolerant stance against CompuServe even though CompuServe does not possess the capability of censorship). In contrast, a much more reasonable action includes giving the ISP notice of the intolerable information and thereafter requesting the removal of the information. See id. See Bovenzi, supra note 109, at 136 (stating a system operator or an ISP's liability should apply only when the ISP knows that an obscene, illegal or defamatory message is posted on the system and the ISP refuses to remove this information).

message to other ISPs stating Singapore requests blockage of the specific United States web site.¹¹⁷ The Singaporean adolescent attempts to use an overseas ISP to access the United States web site but is denied.¹¹⁸

F. The Pros and Cons of Self-regulation and Government Censorship

Self-regulation with PICS gained immediate approval from nations adamant in searching for a solution to curb intolerable information but sensitive to free expression.¹¹⁹ Nevertheless, PICS has its problems. First, implementation of PICS to decrease the international spread of intolerable material depends on international adherence, which is not likely.¹²⁰ Second, when a nation's government takes a self-regulation approach to the Internet, adverse results are inevitable and government instability is a likely result.¹²¹ Third, a related issue to the spread of intolerable information on the Internet.¹²² Self-regulation of the Internet does not address trademark and copyright infringement unless the government entrusts a self-policing system to curb trademark and

119. See Staiman, supra note 95, at 904-905. PICS solves two insurmountable problems which legislation has yet to solve. See *id.* First, the decentralized structure of the Internet lends itself best to regulation at the user's terminal. See *id.* Second, regulation by rating is the least abhorrent to free expression. See *id.*

120. See Hill, supra note 58, at 13 (noting PICS does nothing to stop the traffic of obscene material continuing unabated outside areas that cannot enforce local anti-obscenity laws unless a rating system is implemented internationally); Arthur, supra note 106, at 5 (currently the UK, Australia and the United States are backing rating systems).

121. When a web site is deemed to be obscene a caller informs the ISP and the ISP takes action by removing the web site, however, if the ISP does not remove the web site it may face liability. See Stratton Oakmont, Inc. v. Prodigy Serv. Co., No. 31063/94, 1995 WL 323710 at *6 (N.Y. Sup. Ct. May 24, 1995), for the proposition that an ISP may be held liable for the tort of one its web site clients; Cf. Boston, supra note 112 (depicting the German government's application of a German criminal obscenity law to an ISP official for the crime of a web site owner).

122. See generally Religious Tech. Center v. Netcom On-Line Communication Serv., Inc., 907 F. Supp. 1361, 1367 (N. D. Ca. 1995) (holding an ISP may be found to have contributorily copyright infringed for the copyright violation of a web site owner).

Miller v. California, 413 U.S. 15 (1973) (noting a United States citizen was convicted under California's criminal obscenity statute for distributing sexually explicit books).

^{117.} See Bovenzi, supra note 109, at 140 (noting that if users complain the ISP would be required to intervene and remove the harmful message). Taken one step further the local ISP communicates internationally with other ISPs and the Singaporean adolescent is essentially incapable of accessing the pornographic images.

^{118.} Internet transmissions take only a fraction of a second whereas communications between ISPs may require substantially more time. COMER, *supra* note 63, at 93 (noting Internet packet switching is measured in thousands of seconds and a human being perceives this as instantaneous).

copyright violations.¹²³ Ironically, while the United States and the EU seek to foster their respective economies with their non-regulatory approach, the non-enforceability of trademark and copyright rights actually weakens their respective economies.¹²⁴ Lastly, the Internet is constantly evolving and appending labels to each new web site is an untenable proposition.¹²⁵

Although government censorship resonates a draconian echo in the ears of western civilization,¹²⁶ censorship has proven to be an effective way of regulating information.¹²⁷ The negative side to government censorship is quite apparent. Rather than a lowest common denominator effect, government censorship invokes a limitation effect probably stricter than any lowest common denominator effect.¹²⁸ In addition, government censorship requires immense government efforts and subsidies.¹²⁹ With all this added effort citizens, under this type of regulation,

125. See Hill, supra note 58, at 13 (more than 500 megabytes of new information are added every day which equals 33 times the length of the famous book "War and Peace").

126. See Sainty et al., supra note 98, at 276 (strictly controlled access regimes are unappealing from a Western perspective).

127. See Net Panel Wants Clearer Guidelines, BUS. TIMES (SING.), Sept. 26, 1997. The National Internet Advisory Committee ("NIAC") reported that Singapore's Internet regulation did not hinder usage of the Internet. See id. Moreover, the Singapore Broadcast Authority ("SBA"), Singapore's government entity overseeing Internet regulation, believes Singapore to be a "visionary" to Internet regulation and a pro-active player in the information technology field, keeping abreast of global technology and business trends, yet at the same time addressing public concern by helping to make the Internet safe for all. See id.

128. See Singapore Country Report on Human Rights Practices For 1996, DEPT. OF ST. HUM. RIGHTS COUNTRY REP., Feb. 1997. Singapore invokes a severe limitation on free expression as shown by a recent human rights update stating:

The [Singaporean] government continued to intimidate opposition parties and their candidates and to restrict the independence of the judiciary in cases with political implications or affecting members of the ruling party. The Government has side powers to detain people arbitrarily and subsequently restrict their travel, freedom of speech, and right to associate freely, and to handicap political opposition. There was no evidence of a change in the Government's willingness to restrict these human rights when it deemed that necessary in pursuit of its policy goals. The Government restricts press freedom and intimidates journalists into practicing self-censorship. There is some legal discrimination against women, which affects only a small percentage of the population. The Government has move actively to counter societal discrimination against women and minorities. While freedom of religion is generally respected, the Jehovah's Witness organization has been banned since 1972.

Id.

129. See Censorship and The Internet, supra note 53. Compared to PICS where government essentially takes no part in regulation, the Singaporean government employs censors

^{123.} See generally id. at 1373-74 (the more passive and unknowledgable an ISP becomes about content of its subscribers the less protection a copyright holder can expect).

^{124.} See Doris E. Long, The Protection of Information Technology in a Culturally Diverse Marketplace, 15 J. MARSHALL J. COMPUTER & INFO. L. 129, 149-150 (1996) (stating a government's inability to enforce copyright and trademark rights ultimately leads to an adverse economic impact).

still manage to reach intolerable information by merely contacting an overseas ISP.¹³⁰

Currently, each nation finds it difficult, if not impossible, to control Internet transmissions past its borders, nevertheless, an international effort at Internet regulation may trigger new efforts and technologies.¹³¹ Currently, no regulation system is infallible, however, the appropriate regulatory structure may instill cooperation between nations, support private efforts in furthering technology and allow governments to select a degree of regulation suitable to governmental interest.

The Multinational Approach will first create an international committee to design a flexible regulatory structure. Second, the Multinational Approach will provide each country with discretion to control all the ISPs. Once implemented, the Multinational Approach will move to allow the Internet to remain an international platform for economy, education and technology and reduce the availability of intolerable materials to each nation.

IV. CONCLUSION

The Internet is a powerful international communication network that offers people of each nation the ability to exchange information, ideas and technology in a manner such that the distance between nations become insignificant; the Internet truly is the twentieth century utopian dream. However, there are people like a man from Lakewood, Ohio, recently charged with violating a community obscenity law when he was caught downloading child pornography at a public library.¹³² This incident and many like it are occurring throughout the world.¹³³

132. See Matthew McAllester, NewsBytes / A Pol Pot Net Hoax, NEWSDAY NASSAU AND SUFFOLK ED., July 6, 1997, at A43 (noting James R. Thomas of Strongsville was taken into custody in a Cleveland suburb, charged with the illegal use of a minor in nudity-oriented material and released on a \$5,000 dollar bond when he was caught in the Lakewood, Ohio town library computer accessing an Internet site with pictures of nude boys and loading the images onto a floppy disk).

133. See Hill, supra note 58 (stating that more than 100 people in America were arrested for using the Internet to spread child pornography around the world and more than

to review more than 25,000 pieces per year and the increase in censors is 400% over a ten year span from 1983 to 1993. See id.

^{130.} See Joshi, supra note 78, at C2 (Singaporean's wishing to connect to otherwise inaccessible overseas web site are doing so by using foreign providers and paying international phone charges).

^{131.} Corporations tend to invest significant amounts of revenue in a system they believe will foster economic growth. With the wide spread acceptance of PICS corporations believing PICS to be the regulation of the future are beginning to invest. *Internet Linx Plans to Fund UK Internet Watchdog*, Network Week, Aug. 8, 1997, *available in WESTLAW*, NETWORKWK File (stating that the London Internet Exchange has announced that it will give financial funding to the Internet Watch Foundation (IWF) to promote ISP self-regulation of Internet content in an attempt to avoid government regulation).

People have a fascination¹³⁴ with 'adult material' termed 'obscene' in the United States, however, obscene information has First Amendment protection in the United States. When 'obscene' material loses its constitutional protection, the United States terms this type of information 'indecent' and the government feels the need to eradicate this type of information. Each country has its own definition of 'indecent' or information it deems intolerable.

All nations agree some form of Internet regulation is necessary. On one end of the spectrum is government censorship, all lines of communications are intercepted by the government. On the other end is self-regulation, leaving parents the task of establishing the comfortable rating to meet family viewing standards. These two guideposts stand unchallenged, unfortunately, there remains nothing in the middle and the two ends do not recognize each other.

Nations share a common goal: reducing intolerable information on the Internet. On this platform an international effort may be formed. An incremental step further includes designing the architecture of a flexible system which supports both government censorship and self-regulation with the common thread being government control over ISPs. This cooperation is likely to cause a chain reaction resulting in a technological focus directed toward ISP communication rather than beefed up in-home regulation or extravagant government technology.

Stymied legislative bodies find the Internet difficult to regulate, however, the present hands off approach is creating a mockery of well established law.¹³⁵ Each country connected to the Internet may opt to

134. 48% of Germans Want More Porn Films On TV, CHI. TRIB., Nov. 15, 1997, § 1, at 23 (the Emnid institute found that nearly half of German TV viewers would like to see more porn films); see also Censorship in the Land of the Free, supra note 133 (noting a United States research team found users in diverse locations accessing pornography sites).

135. See Bovenzi, supra note 109, at 127. The posting of information on a web site is analogized with the publishing of written materials. See id. A publisher of written materials is generally liable for obscene materials it publishes, however an ISP is not liable for allowing obscene materials on the Internet since the ISP is a passive conduit and cannot be found liable in the absence of fault. See id. See Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710 *8 (N.Y. Sup. Ct. May 24, 1995). The court held that an ISP is not merely a passive transmitter of information, but essentially a publisher, responsible for the content of material posted on its electronic bulletin boards. See id. In Cubby, Inc. v. CompuServe, 776 F. Supp. 135 (S.D.N.Y 1991), the court reached exactly the opposite decision. See id. However both courts analyzed the ISPs control over the information available on the system in order to estimate ISP liability. Id. at 143.

^{200,000} pornographic images of children as young as 18 months were found by investigators); see Censorship in the Land of the Free, DataQuest (India), Mar. 15, 1997, available in WESTLAW, DATAQUEST File (stating a United States research team was able to identify consumers of paraphilic and pedophilic computer pornography from countries as diverse as China, Saudi Arabia, Turkey, South Africa, Chile, Malaysia, Hungary, Trinidad, Tobago, New Zealand, Hong Kong, Nigeria, and Japan).

1024 JOURNAL OF COMPUTER & INFORMATION LAW [Vol. XVI

either ignore Internet regulation or implement a system that supports an international scope and uphold each nations established jurisprudence.

Steven M. Hanley