

Fordham International Law Journal

Volume 20, Issue 3

1996

Article 9

Shielding Internet Users from Undesirable Content: The Advantages of a Pics Based Rating System

Ari Staiman*

*

Copyright ©1996 by the authors. *Fordham International Law Journal* is produced by The Berkeley Electronic Press (bepress). <http://ir.lawnet.fordham.edu/ilj>

Shielding Internet Users from Undesirable Content: The Advantages of a PICS Based Rating System

Ari Staiman

Abstract

This Note argues that the European Union should adopt the Commission recommended a Platform for Internet Content Selection ("PICS") based rating system because the PICS based rating system is the most technically and legally effective method for combating undesirable content on the Internet and because it furthers freedom of expression as well as the European Union common market's four freedoms. Only a coordinated worldwide system, furthermore, will enable the European Union and governments throughout the world to effectively shield citizens from undesirable content, regardless of how a particular government may define the term undesirable. This Note, therefore, argues that governments of the world should implement a global PICS based rating system. Part I briefly describes the Internet and continues by discussing the European Union and several European Union policies related to Internet regulation. Part II examines attempts at shielding citizens from undesirable Internet content by the European Union and its Member States, as well as attempts by several countries that are not part of the European Union. Part III argues that the PICS based rating system is both technologically and legally the most suitable way for the European Union to shield citizens from undesirable Internet content. Part III also proposes a global rating system, based on the European Union PICS based rating system, which will enable the European Union and governments throughout the world to effectively protect citizens from undesirable content on the Internet. This Note concludes that the proposed global PICS based rating system will enable a government that uses it to protect its citizens from undesirable Internet content in a way that is consistent with that government's particular legal system.

NOTES

SHIELDING INTERNET USERS FROM UNDESIRABLE CONTENT: THE ADVANTAGES OF A PICS BASED RATING SYSTEM

*Ari Staiman**

"We know that national regulation [of the Internet] is not enough, that European regulation is not enough We may need to have a world regulation of these matters."¹

INTRODUCTION

The Internet² contains a wide variety of content,³ ranging

* J.D. Candidate, 1998, Fordham University.

1. *Commission Green Paper to Broach Porn on the Internet*, Reuter European Community Report, Sept. 24, 1996, available in LEXIS, EURCOM Library, REUEC File.

2. See Richard Dennis, *Guide to Selecting an Internet Provider*, 2 ENVTL. L. 571, 572-73 (1996) (defining Internet as network that connects networks throughout world, often described as "a network of networks."). A network is a system consisting of any combination of computers, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment. Anthony Cataldo, *IBM Eyes Embedded Market: Hedging Against Possible Loss of Apple to Intel*, ELECTRONIC BUYERS' NEWS, Mar. 3, 1997, at 16. A dedicated broadband telecommunications connection, known as the backbone, linking together host computers comprises the Internet. Cris Shipley & Matthew Fish, *The Web and the Internet*, COMPUTER LIFE, Oct. 1, 1996, at 115. A dedicated connection is one that is always active. *Id.* A broadband connection is one that can transmit large amounts of data simultaneously. *Id.* Host computers are computers that maintain a connection to the backbone. *Id.* These host computers are part of a network and maintain connections to other computers that, in turn, maintain connections to other computers. *Id.* Computers join the network via dedicated telephone lines or, as is typical with users from home, through home telephones. *Id.*

3. See Michael Krantz, *Wired for Sound: Rock 'N' Roll Is Exploding on the Internet*, TIME, Dec. 2, 1996, at 74 (detailing that users can listen to concerts on Internet); Richard Zoglin, *The News Wars on TV and Radio, In Print and Over the Internet*, TIME, Oct. 21, 1996, at 58 (noting that users can find newspapers published on Internet); *Porn Pirates and Software Smugglers*, TIME, July 25, 1994, at 18 ("[t]ens of thousands of illicit computer-porn sites now litter the [Internet]."); *Space Watch, Cyberstyle*, TIME, July 25, 1994, at 18 (stating "[s]pace fans eager to join in the moon-landing anniversary celebrations or hear the latest shuttle updates can get news about the space agency on the [Internet]."); Alan Boyle, *7 Deadly Sins on the Internet*, MSNBC (visited Oct. 18, 1996) <<http://www.msnbc.com/news/30680.asp>> (also on file with the *Fordham International Law Journal*) (detailing types of Internet content, including sexually explicit and violent content and content that infringes copyrights).

from Mozart's operas⁴ to information on making bombs,⁵ and from medical advice on cancer or heart disease⁶ to sexually explicit materials.⁷ Citizens around the world are accessing the Internet,⁸ with estimates placing the current number of Internet users⁹ ("users") as high as forty million.¹⁰ The European Union¹¹ Commission of the European Communities¹² ("Com-

4. Welton Jones, *Classical Passion on the Internet*, SAN DIEGO UNION-TRIB., at 25 (discussing where to find Mozart operas on Internet).

5. Eric Lichtblau & Jim Newton, *Internet Cited for Surge in Bomb Reports*, L.A. TIMES, June 27, 1996, at B1 (reporting on bomb making information on Internet). Los Angeles explosives experts, including the Los Angeles police department, contend that a recent significant rise in bomb scares is due to users retrieving bomb-making technology from the Internet. *Id.*

6. See Eryn Brown, *Where to Find Medical Advice On The Web*, FORTUNE MAGAZINE, at 162 (discussing availability of medical advice on Internet).

7. See Geeta Anand, *Library Internet Censoring Planned Hub Orders Software to Block Pornography*, BOSTON GLOBE, at B1 (noting children are accessing sexually explicit content on Internet from libraries).

8. Shea ex rel. American Reporter v. Reno, 930 F. Supp. 916, 926 (S.D.N.Y. 1996).

9. See Tim Blangger, *Questions Remain Despite Shift in Encryption Control*, MORNING CALL, Dec. 3, 1996, at D01 (defining users as people who access Internet).

10. Shea ex rel. American Reporter, 930 F. Supp. at 926.

11. Treaty on European Union, Feb. 7, 1992, art. A, O.J. C 224/1 (1992), [1992] 1 C.M.L.R. 719, 31 I.L.M. 247 [hereinafter TEU] (amending Treaty Establishing the European Economic Community, Mar. 25, 1957, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1 (Cmd. 5179 -II) [hereinafter EEC Treaty], as amended by Single European Act, O.J. L 169/1 (1987), [1987] 2 C.M.L.R. 741 [hereinafter SEA], in TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987)). Until 1995, the twelve European Union ("EU") Member States were Belgium, Denmark, France, Germany, Greece, Spain, Ireland, Italy, Luxembourg, the Netherlands, Portugal, and the United Kingdom. TEU, *supra*, pmbl., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725-26. On January 1, 1995, Austria, Finland, and Sweden became EU Member States. *The European Commission: The Week in Europe — Week Ending 31 May 1996*, M2 PRESSWIRE, June 7, 1996, available in WESTLAW, Allnewsplus Database.

12. See Treaty Establishing the European Community, Feb. 7, 1992, [1992] 1 C.M.L.R. 573 [hereinafter EC Treaty], incorporating changes made by TEU, *supra* note 11, art. 155, [1992] 1 C.M.L.R. at 682 (describing Commission of European Communities' ("Commission") duties in enforcement of EU policy); ANDREW EVANS, THE LAW OF THE EUROPEAN COMMUNITY INCLUDING THE EEA AGREEMENT 7 (1st ed. 1994) (analogizing Commission to "government, in that it draws up legislative proposals and is responsible for supervising application of resulting legislation and for implementation of Community budget."). The Commission performs executive functions implementing and enforcing EU legislation. A.G. TOTH, THE OXFORD ENCYCLOPAEDIA OF EUROPEAN COMMUNITY LAW 70 (1990). The Commission's activities include formulating legislative proposals for new policies, supervising application of the resulting legislation by mediating between the Member states, and for overseeing the proper execution of existing EU policies. See Evans, *supra*, at 14-15 (noting that Article 155 of EC Treaty requires Commission to act against violations of EU law and that EC Treaty requires Commission to formulate recommendations or deliver opinions on matters dealt with in Treaty); T.C. HARTLEY, THE FOUNDATIONS OF EUROPEAN COMMUNITY LAW: AN INTRODUCTION TO THE

mission") has noted that the Internet has become essential in attaining and transferring information globally¹³ and exerts social, educational, cultural, and economic influence.¹⁴

During the past year, EU Member States have been grappling with the question of how best to shield their citizens from undesirable content¹⁵ on the Internet.¹⁶ Member states have been concerned with protecting children from Internet content that may be inappropriate for them as well as with preventing all users from accessing illegal Internet content.¹⁷ In October 1996, the Commission put forth recommendations for combating undesirable content on the Internet, including backing a rating system¹⁸ based on the Platform for Internet Content Selection¹⁹ ("PICS") that would allow parents, educators, and others to de-

CONSTITUTIONAL AND ADMINISTRATIVE LAW OF THE EUROPEAN COMMUNITY 11 (3d ed. 1994) (categorizing supervision of resulting legislation as one of "most important activities" of Commission). The Commission also is responsible for the proper functioning and development of a common EU market. EC Treaty, *supra* note 12, art. 155, [1992] 1 C.M.L.R. at 682.

13. See Commission Communication, COM (96) 487 (1996) (to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Illegal and Harmful Content on the Internet) at 3 (stating "the Internet has established itself as one of the main building blocks of the Global Information Infrastructure . . . in Europe.").

14. See *id.* ("the Internet has become a powerful influence in the social, educational and cultural fields.").

15. *Shea ex rel. American Reporter*, 930 F. Supp. at 925, n.2 (defining content as any text, data, sound, computer program, or visual image exchanged on Internet); Commission on the European Communities, Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services: Green Paper from the Commission to the European Council, COM (96) 483 Final (1996), at 6 [hereinafter Green Paper] (explaining that undesirable content may be either illegal content or content that some segment of society would find harmful or objectionable).

16. See *A Land of New Media Apathy*, NEW MEDIA AGE, Aug. 1, 1996, at 8 [hereinafter *A Land of New Media Apathy*] (discussing German police request that CompuServe block transmission of pornographic newsgroups on Internet); *Banned President Mitterand Book Posted Online*, NEWSBYTES NEWS NETWORK, Jan. 25, 1996, at 2 [hereinafter *Banned President Mitterand Book*] (detailing France's actions in removing banned French book from Internet); John Minson, *No Time For a New Law; Current Obscenity Laws Are No Way to Control the Net*, GUARDIAN, Sept. 12, 1996, at 2 (discussing U.K. Government hinting at arrests if ISPs did not prevent access to newsgroups containing illegal content);

17. Natasha Wanchek, *Nations Consider Internet Regulations*, UNITED PRESS INT'L, May 3, 1996 available in LEXIS, News Library, Curnws File; *supra* note 16 and accompanying text (detailing German, French, and U.K. efforts to regulate Internet).

18. See Arman Danesh, *Net Nannies Raise Protective Screens*, S. CHINA MORNING POST, Oct. 29, 1996, at 2 (defining rating as labeling content based on any number of criteria such as nudity and violence); *Internet Access Controls Without Censorship*, PICS (last visited Oct. 22, 1996) <<http://www.w3.org/pub/WWW/PICS/iacwcv2.htm>> (also on file with the *Fordham International Law Journal*) (defining rating Internet content as process of

termine the type of content minors may access on the Internet.²⁰ The Commission contended that attaining the goal of protecting Internet users from undesirable Internet content requires a unified EU implementation of PICS and, perhaps, a worldwide implementation.²¹

This Note argues that the European Union should adopt the Commission recommended PICS based rating system because the PICS based rating system is the most technically and legally effective method for combating undesirable content on the Internet and because it furthers freedom of expression²² as well as the EU common market's²³ four freedoms.²⁴ Only a coordinated worldwide system, furthermore, will enable the European Union and governments throughout the world to effectively shield citizens from undesirable content, regardless of how a particular government may define the term undesirable. This Note, therefore, argues that governments of the world should implement a global PICS based rating system. Part I briefly describes the Internet and continues by discussing the European

using term or set of terms to describe type or category of content, for example, rating of "XXX" denoting sexually explicit content).

19. *Net Shepherd Releases New Technology That Collaboratively Rates and Filters the Internet Software Is First to Comply with New Industry Established Standards (PICS)*, CANADA NEWSWIRE, July 30, 1996, available in WESTLAW, Allnewsplus Database (noting that Platform For Internet Content Exchange ("PICS") is series of technical specifications that provide Internet standards for rating formats).

20. See Commission Communication, *supra* note 13, COM (96) 487, at 18-24 (discussing Commission's recommendations concerning undesirable Internet content).

21. See *id.* at 5 (positing that undesirable content on Internet calls for "response at EU and international level.").

22. TEU, *supra* note 11, art. F(2), O.J. C 224/1, at 99. Article F(2) of the TEU states:

The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member State, as general principles of Community law.

Id. Freedom of expression is included in the scope of Article F(2). See Green Paper, *supra* note 15, COM (96) 483 Final at 32 (providing legal background of right to freedom of expression in European Union).

23. See EC Treaty, *supra* note 12, art. 2, [1992] 1 C.M.L.R. at 588 (asserting that European Community shall establish a common market and that common market shall provide principal medium to achieve Community functions).

24. See EC Treaty, *supra* note 12, art. 3, [1992] 1 C.M.L.R. at 588 (providing that activities of Community shall include "an internal market characterized by the abolition, as between Member States, of obstacles to the [four freedoms of] free movement of goods, persons, services and capital.").

Union and several EU policies related to Internet regulation. Part II examines attempts at shielding citizens from undesirable Internet content by the European Union and its Member States, as well as attempts by several countries that are not part of the European Union. Part III argues that the PICS based rating system is both technologically and legally the most suitable way for the European Union to shield citizens from undesirable Internet content. Part III also proposes a global rating system, based on the EU PICS based rating system, which will enable the European Union and governments throughout the world to effectively protect citizens from undesirable content on the Internet. This Note concludes that the proposed global PICS based rating system will enable a government that uses it to protect its citizens from undesirable Internet content in a way that is consistent with that government's particular legal system.

I. INTERNET AND THE EUROPEAN UNION DESCRIBED

Although what was to become the Internet started in 1969,²⁵ non-scientists did not play an active role in it until the European Particle Physics Laboratory²⁶ ("CERN") developed the World Wide Web²⁷ ("WWW") in 1989.²⁸ Users employ many types of

25. NICHOLAS NEGROPONTE, BEING DIGITAL 233-34 (1996) (explaining that Internet began as experimental computer network set-up by U.S. defense department during peak of Cold War).

26. Gail Edmondson, *Surprise! Europe Is Finally Getting Its Software Act Together—And Going After America's Lead*, BUS. WK., May 6, 1996, at 34. The European Particle Physics Laboratory ("CERN"), which developed the World Wide Web ("WWW"), is a nuclear research organization located in Switzerland. *Id.* CERN is the French acronym for the European Laboratory for Particle Physics. Shipley & Fish, *supra* note 2, at 115.

27. Shipley & Fish, *supra* note 2, at 115. The WWW is a system that exchanges information between users' computers and a server so users can share information on a network. *Id.* A server consists of software that allows a computer to offer a service to another computer and the computer on which the server software runs. Dennis, *supra* note 2, at 586. Software consists of programs used to direct the operation of a computer. *Id.* Users exchange information on the WWW through web pages, a file on a computer directly connected to the Internet by servers. Charles Waltner, *Internet Hits and Errors*, MULTICHANNEL NEWS, Mar. 25, 1996, at 40B. Hypertext Markup Language ("HTML") the programming language used to create most web pages, allows content providers to link Web pages together in a web-like fashion. See Shipley & Fish, *supra* note 2, at 115 (discussing HTML). By clicking on these hyperlinks, represented by words or pictures, users can jump from one web page to another, even if stored on a different server. See *id.* (discussing hyperlinks).

28. See *British Minister Opens CERN World Wide Web Days*, M2 PRESSWIRE, Mar. 30, 1995, available in WESTLAW, Allnewsplus Database [hereinafter *British Minister Opens*] (noting that WWW "has transformed the Internet from a tool for academics and com-

technologies to exchange desirable and undesirable content on the Internet.²⁹ The Internet is an international system with no centralized control over the types of content transmitted on it.³⁰ Consequently, attempts to identify and control undesirable Internet content have been mostly technology-based, as opposed to centralized, government imposed content regulations by such alliances as the European Union.³¹

A. History of the Internet

In 1969, the U.S. Department of Defense's Advanced Research Projects Administration³² established the ARPANet,³³ a

puter buffs into a vast reservoir of information which anyone can use."); Herb Brody, *The Web Maestro: An Interview with Tim Berners-Lee*, *TECH. REV.* July 1, 1996, at 33 (stating "so powerful is the appeal of the graphics and hyperlinks that newcomers to the online world might be forgiven for thinking that the Web is the Internet, rather than just an especially powerful and convenient way to navigate through the worldwide collection of networked computers."); Kathy Yakal, *The Day the 'Net Went Down'*, *ELECTRONIC INVESTOR*, June 24, 1996, at 24 (stating "with the creation of the World Wide Web by Tim Berners-Lee at the CERN nuclear research center in Geneva in 1989, the [Internet] blossomed into the graphics- and link-rich environment that's emerging today.").

29. See Karen S. Frank, *Potential Liability on the Internet*, 437 *PLI/PAT* 417, 424-25 (1996) (detailing technologies used for content exchange, including electronic mail ("e-mail"), Usenet, real-time communications, and WWW). E-mail consists of "messages from one individual to another sent via telecommunication links between computers or terminals." *Id.* Usenet is a series of networks on the Internet where users can place messages into topical groups, called newsgroups. DANIEL P. DERN, *THE INTERNET GUIDE FOR NEW USERS* 196 (1994). Real Time communications allow users to engage in immediate dialogue with others on the Internet. *American Civil Liberties Union*, 929 F. Supp. 824, 835 (E.D. Pa 1996).

30. See Randolph Stuart Sergent, *The "Hamlet" Fallacy: Computer Networks and the Geographic Roots of Obscenity Regulation*, 23 *HASTINGS CONST. L.Q.* 671, 676 (1996) (discussing Internet's lack of central control). The Internet has no center and each computer added to the Internet becomes a parallel part of the overall network. Wendy Grossman, *All You Never Knew About the Net . . .*, *INDEPENDENT*, July 15, 1996, at 15. Any computer can connect to the Internet as long as it uses set protocols. *Id.* A protocol is how computers communicate. *British Minister Opens*, *supra* note 28.

31. Sara Woodard, *Living Out Of Site, Out Of Mind It's 10 P.M. Do You Know What Your Kids Are Doing On The Internet*, *NEW ORLEANS TIMES-PICAYUNE*, Jan. 5, 1997, at C1 (discussing technology-based control of Internet access as opposed to governmental control).

32. Edwin Diamond et al., *The Ancient History of the Internet*, *AM. HERITAGE*, Oct. 1, 1995, at 34. The U.S. Department of Defense created the Advanced Research Projects Agency ("ARPA") during the Cold War, charging it with allotting funds for high-tech research. *Id.* ARPA's priorities included military projects on command, control, and communication. *Id.*

33. *Id.* ARPANet is an acronym for Advance Research Projects Administration Network. *Id.* ARPA funded ARPANet to test the feasibility of using computers from the battlefield, to test the feasibility of a communication network that the military could use

computer network³⁴ enabling reliable transmissions of communications between institutions conducting U.S. defense-related research.³⁵ ARPANet implemented a process called "packet-switching"³⁶ to preserve the network's operability in the event of an enemy attack.³⁷ Packet-switching is a process by which a computer divides a message sent from one computer to another into separate pieces of data, known as packets.³⁸ Each packet takes a different route, along different computers and networks, to the ultimate destination computer, which reassembles the total message.³⁹ If part of the network becomes inoperable, due, for example, to a nuclear attack, this process automatically reroutes the packet through a different path to the ultimate destination computer.⁴⁰

during and after a nuclear World War, and to enable researchers throughout the country to share computers so that the Department of the Defense could save money. *Id.* At the time that ARPA established ARPANet, computers were large and expensive, with one computer often taking up an entire room. *Where Wizards Stay Up Late: The Origin of the Internet*, PUBLISHERS WKLY, July 15, 1996, at 65 [hereinafter *Where Wizards Stay*]. These computers were unable to communicate with other computers. *Id.*

34. See Cataldo, *supra* note 2, at 1290 (defining network).

35. *Shea ex rel. American Reporter*, 930 F. Supp. at 925-26.

36. *Where Wizards Stay*, *supra* note 33, at 65. British Scientist Donald Davies and U.S. scientist Paul Baran devised the packet-switching technology. *Id.*

37. Peter Golding, *World Wide Wedge: Division and Contradiction in the Global Information Infrastructure*, MONTHLY REV., July 17, 1996, at 5-6. The U.S. Department of Defense embraced the idea of packet-switching during the cold war to prevent a nuclear strike from disabling U.S. military computer capability. Shipley & Fish, *supra* note 2, at 115.

38. Diamond, et al., *supra* note 32, at 34.

39. Golding, *supra* note 37, at 70. The process of sending information directly between two computers would have been much quicker than packet switching, because packets do not always take the most direct route to the destination. *Id.* Packet switching, however, allowed for decentralized control, circumventing centralized control centers that are more vulnerable to military attack. Diamond, et al., *supra* note 32, at 9.

40. *Shea ex rel. American Reporter*, 930 F. Supp. at 926; *American Civil Liberties Union*, 929 F. Supp. at 832. One illustration of packet switching states:

Pretend I (in Boston) am sending you (in San Francisco) this paragraph. Each Packet (containing, say ten letters, its sequence number, plus your name and address) can in principle take a different route, one via Denver, one via Chicago, one via Dallas, and so on. Imagine now, when they line up in San Francisco, they discover that packet six is missing So let's pretend that packet six went through Minneapolis, which, at the very same moment, was struck by an enemy missile. Packet six was lost. As soon as packet six is determined to be missing, the other packets ask Boston to resend it (not via Minneapolis this time). This means that to stop a message from getting from me to you, one needs to wipe out most of America, as there will always be an available path of some sort.

Negroponte, *supra* note 25, at 234.

Over time, different institutions added networks to ARPANet and, through the added networks, connected individuals around the world.⁴¹ By 1982, the term Internet emerged to describe ARPANet and the added networks.⁴² The number of host computers⁴³ connected directly to the Internet reached 10,000 by 1987, 100,000 by 1989, and 1,000,000 by 1991.⁴⁴ Estimates place the current number of users as high as forty million,⁴⁵ with that figure expected to grow to 200 million by the year 1999.⁴⁶

Tim Berners-Lee, a U.K. national, supervised CERN's development of the WWW in 1989⁴⁷ to allow physicists around the world to collaborate and publish papers.⁴⁸ Berners-Lee introduced the concept of hypertext transfer protocol⁴⁹ ("http") which enables users' computers to present different types of content together on one document, known as a web page.⁵⁰ The information provided in web pages is not limited to text and graphics, but can take the form of any type of content.⁵¹ Http

41. See *History of the Internet*, KAN. CITY STAR, Apr. 21, 1996, at 2 [hereinafter *History of the Internet*] (noting continuous increase in Internet users over time).

42. *Id.*

43. See Shipley & Fish, *supra* note 2, at 115 (defining host computers).

44. *History of the Internet*, *supra* note 41, at 3.

45. *Shea ex rel. American Reporter*, 930 F. Supp. at 926.

46. See *American Civil Liberties Union*, 929 F. Supp. at 831 (discussing exponential growth of Internet).

47. Jack Schofield, *Berners-Lee Goes for a Gong He Wrote the Programs, Protocols and Languages That Make the World-Wide Web Tick*, GUARDIAN, July 11, 1996, at 5. Although Berners-Lee developed the WWW in October 1990, he did not release it inside CERN until December 1990 and did not place it on the Internet until 1991. *Id.*

48. *History of the Internet*, *supra* note 41, at vii; Philip Manchester, *A-Z of the Internet: Cern is a Natural Melting Pot for a Wide Range of Leading Edge Technologies*, FIN. TIMES, Apr. 3, 1996, at 1.

49. See *British Minister Opens*, *supra* note 28 (noting that hypertext transfer protocol ("http") allows linkage of related pieces of information on computers, and providing example of user seeing highlighted word or phrase and using mouse to choose word or phrase to access additional information).

50. Eugene Volokh, *Computer Media for the Legal Profession*, 94 MICH. L. REV. 2058, 2062 (1996). Entities maintaining web pages sometimes sell advertising on them. *American Civil Liberties Union*, 929 F. Supp. at 847. Such entities depend on a demonstration that the sites are widely available and frequently visited to secure advertising revenue. *Id.*

51. EDUCATOR'S GUIDE TO THE INTERNET 219 (Mary Sandy ed., 1997) [hereinafter EDUCATOR'S GUIDE]. See Shipley & Fish, *supra* note 2, at 115 (discussing that content providers can include computer programs in their web pages, for example, bank could include calculator in web page).

also allows users to interact with web pages through hyperlinks.⁵² By choosing hyperlinks from web pages, a user's computer automatically locates and displays different parts of the same web page or completely different web pages.⁵³ The WWW thus enables users to access additional web pages from initial web pages without typing anything into the computer and without knowledge of which computer on the Internet contains the additional web pages.⁵⁴

By the beginning of 1993, there were approximately 50 servers for the WWW.⁵⁵ Today, there are over 100,000 servers.⁵⁶ Computer historians credit the WWW, due to its graphical and interactive nature, with changing the Internet from something that only scientists used to something that non-scientists find useful.⁵⁷

In order to maintain standards for the WWW, CERN established the World Wide Web Consortium⁵⁸ ("W3C") in collaboration with the U.S. Defense Advanced Research Projects Agency⁵⁹ ("DARPA") and the Commission.⁶⁰ Today, W3C continues to draw international support, with sponsors including the Massachusetts Institute of Technology Laboratory for Computer Science,⁶¹ the French National Institute for Research in Computer

52. *British Minister Opens*, *supra* note 28. Hyperlinks, represented on a user's computer screen by highlighted or underlined words or pictures, interact with the Internet's communications protocols to connect to web pages on one host computer to web pages on the same or another host computer. Shipley & Fish, *supra* note 2, at 115.

53. *Shea ex rel. American Reporter*, 930 F. Supp. at 929.

54. Shipley & Fish, *supra* note 2, at 115.

55. Schofield, *supra* note 47, at 5.

56. *Id.*

57. *Id.*; see *supra* note 28 and accompanying text (relating computer historians' views that Internet expansion resulted from WWW introduction).

58. See Ben Rooney, *Connected: Computer World Hails "Mr. Web"*, DAILY TELEGRAPH LONDON, July 23, 1996, at 2 (noting that World Wide Web Consortium's ("W3C") mission is to realize full potential of WWW); Grossman, *supra* note 30, at 15 (discussing that W3C, rather than major computer corporations, shapes development of WWW).

59. *Digital Market Announces Its Selection for Funding by Government's Defense Advanced Research Project Agency*, BUS. WIRE, Nov. 18, 1996, available in WESTLAW, Allnewsplus Database (noting that Defense Advanced Research Projects Agency ("DARPA") is U.S. Department of Defense's central research and development organization). In 1972, ARPA changed its name to DARPA, adding the "D" for defense. Diamond, et al., *supra* note 32, at 13.

60. Commission Communication, *supra* note 13, COM (96) 487, at 21 n.21; W3C, *The World Wide Web Consortium*, (last updated Sept. 19, 1996) <<http://www.w3.org/pub/WWW/Consortium>> (also on file with the *Fordham International Law Journal*).

61. *Apple Computer: Apple joins the World Wide Web Consortium*, M2 PRESSWIRE, Mar. 2,

Science and Control⁶² ("INRIA"), and Japan's Keio University.⁶³ The W3C currently works on new projects to make the WWW more efficient.⁶⁴

B. Internet Content Exchange Technologies

Users can access the Internet either through their own direct Internet connections or through connections of others, including connections of Internet service providers ("ISP").⁶⁵ Any user connected to the Internet may either transmit or receive content.⁶⁶ Users exchange content on the Internet in the form

1996, available in WESTLAW, Allnewsplus Database. Massachusetts Institute of Technology Laboratory for Computer Science's mission is to invent, develop, and understand information technologies. *W3C Issues PICS as a Recommendation*, BUS. WIRE, Dec. 3, 1996, at 5, available in WESTLAW, Allnewsplus Database [hereinafter *W3C Issues PICS*]. It pioneered efforts in interactive computing and computer networking. *Id.*

62. *W3C Issues PICS*, *supra* note 61. *Institut National de Recherche en Informatique et en Automatique* ("INRIA"), the French National Institute for Research in Computer Science and Control, conducts both fundamental and applied research, transfers research results to the computer industry, and is currently researching information processing, advanced high speed networking, structured documents, and scientific computation. *Id.* INRIA has five research units located at Rocquencourt, Rennes, Sophia Antipolis, Nancy, and Grenoble. *Id.*

63. *Web Body Seeks Asian Host*, NEWSBYTES, Oct. 17, 1996, at 2; W3C, *Keio University Joins*, (visited Sept. 25, 1996) <<http://www.w3.org/pub/WWW/Press/Keio-PR.html>> (also on file with the *Fordham International Law Journal*). Keio University, which has five campuses in Tokyo, is one of the oldest private universities in Japan, and is one of Japan's foremost computer science research laboratories. *W3C Issues PICS*, *supra* note 61. Keio University takes part in joint projects with industry and government organizations researching network and digital media technology. *Id.* Keio University has only hosted the project since September 1996. *Id.*; *American Civil Liberties Union*, 929 F. Supp. at 838-39 (providing full list of W3C participants). Participants of W3C include many major Internet Service Providers, hardware and software companies, Internet content providers, and consumer organizations. *Id.*

64. Grossman, *supra* note 30, at 15. W3C is currently working on ways, for example, to store content coming from one country on a server in a second country for temporary retrieval by residents of the second country, to speed up access to the content in the second country. *Id.*

65. See Commission Communication, *supra* note 13, COM (96) 487, at 18-24 (discussing recommendations). The term Internet Service Provider ("ISP") refers generically to organizations providing access to the Internet. *Id.* at 8. Other terms that refer to organizations providing access to the Internet include On-Line Service Providers and, simply, access providers. *Id.*

66. See *Shea ex rel. American Reporter*, 930 F. Supp. at 929-30 (relating relative ease of putting content on Internet). Posting refers to sending content to usenet. Dennis, *supra* note 2, at 586; see Dern, *supra* note 29, at 196 (defining Usenet as series of networks on Internet where users can place messages into topical groups, known as newsgroups).

of text, images, sounds, or computer programs.⁶⁷ Users employ several types of technologies for exchanging content on the Internet, including e-mail,⁶⁸ real-time communication,⁶⁹ Usenet,⁷⁰ File-Transfer Protocol⁷¹ ("FTP"), and the WWW.⁷²

1. E-mail

E-mail, the most widely used Internet technology, allows users to transmit content to other users.⁷³ Knowing a particular e-mail address⁷⁴ does not necessarily⁷⁵ provide information about the person using that address.⁷⁶ No directory exists to

67. Boyle, *supra* note 3 (discussing types of Internet content).

68. See Frank, *supra* note 29, at 424-25 (defining e-mail).

69. *Id.* (defining real-time communication)

70. See Dern, *supra* note 29, at 196 (defining Usenet as multiple networks on Internet where users can place messages into topical groups, called newsgroups).

71. Dominic Andreano, *Cyberspace: How Decent Is the Decency Act*, 8 ST. THOMAS L. REV. 593, 596 (1996). File-Transfer Protocol ("FTP") is a protocol enabling users to exchange content with other computers connected to the Internet. *Id.*

72. See Henry H. Perritt, Jr., *Basic Technological Terms and Concepts*, 443 PLI/PAT 23, 27-28 (1996) (discussing content exchange technologies including e-mail, Usenet, real-time communication, and WWW).

73. See Diamond, et al., *supra* note 32, at 34 (stating "E-mail, of course, is the most widely used of the [Internet] services, the most convenient and the most functional."). E-mail usually travels as several packets of information, which a computer reassembles into the original form at its final destination. Negroponte, *supra* note 25, at 234; see *supra* note 39 and accompanying text (detailing packet switching-technology).

74. *American Civil Liberties Union*, 929 F. Supp. at 847. When users send content over the Internet, they must provide a destination, referred to as an address, that is specific to the message's intended recipient and that other users use to retrieve that content. *Id.* Every address has two parts. Dern, *supra* note 29, at 69. One part identifies the network on the Internet and the other part identifies a particular computer on the network. *Id.* Computers display addresses either as numbers, referred to as an IP address, or as alphanumeric fields, referred to as domain names. *Id.* at 73. Domain names, which consist of two or more alphanumeric fields separated by periods, do not necessarily provide information about users. *Id.* Some fields, however, may indicate an address' country of origin or whether a government, commercial, or educational institution uses the address. *Id.* at 74. A Uniform Resource Locator ("URL") is an address structure the WWW uses to access a specific server and file on the server. EDUCATOR'S GUIDE, *supra* note 51, at 219. URLs can invoke the http protocol on the WWW as well as FTP and Usenet. *Id.*

75. See Dern, *supra* note 29, at 69 (discussing potential anonymity of e-mail addresses).

76. *Shea ex rel. American Reporter*, 930 F. Supp. at 927; *American Civil Liberties Union*, 929 F. Supp. at 845. An e-mail address would provide a user's name only if the user chooses to use his or her name in the e-mail address. *Id.* A user may use an e-mail "alias" or an anonymous remailer, a service that converts e-mail return addresses to pseudonyms and renders the mail untraceable, to completely hide the user's identity. *Id.*

match all e-mail addresses with particular users,⁷⁷ and users can also avoid disclosing their true e-mail addresses by using anonymous remailers or aliases.⁷⁸

2. Real-Time Communication

Real-time communication enables users to engage in conversations with other users on the Internet.⁷⁹ This technology enables users to communicate directly, either by typing messages through internet relay chat ("IRC")⁸⁰ or by speaking directly to other users through Internet telephony.⁸¹ IRC allows multiple users to communicate simultaneously, all seeing what other users type into the computer.⁸² Internet telephony allows users to communicate on the Internet in the way one would use a telephone, except that with Internet telephony, users speak into a microphone attached to their computers.⁸³ Using Internet te-

77. See Dern, *supra* note 29, at 71 (arguing that lack of comprehensive directory of Internet addresses is one of biggest obstacles to using Internet).

78. Shea *ex rel. American Reporter*, 930 F. Supp. at 927. Users, for example, can send e-mail via an anonymous remailer. *Id.*

79. See *American Civil Liberties Union*, 929 F. Supp. at 835 (explaining that real time communications allow user to communicate in "real time," carrying on conversations as one would over telephone).

80. Frank, *supra* note 29, at 425. Internet Relay Chat ("IRC") enables two or more users to communicate. *Id.* IRC is a collection of several networks connected to the Internet that enables servers to send text messages to other servers connected to the networks. Tim Blangger, *Basics Of IRC, the World's Chat Room*, BUFFALO NEWS, Nov. 12, 1996, at D10. The three main IRC networks are Eris Free Net, which approximately 15,000 users may employ at any one time and is the largest of the IRC networks, Undernet, which can accommodate about 10,000 users, and Dalnet, which can accommodate about 5000 users. *Id.* To communicate using IRC, users need to be using the same network and the same channel of the network. *Id.* A channel is a specific part of a network. *Id.*

81. See John M. Moran, *Your PC Is Ringing the Computer Becomes a Telephone, Too*, BUFFALO NEWS, Oct. 15, 1996, at D9 (noting that Internet telephony refers to technology that allows making of telephone calls through computers on Internet). The sound quality of Internet telephony is not as good as that on a telephone. Stephan Somogyi, *Internet Telephony Programs*, MACUSER, Jan. 1, 1997, at 2. Technology also exists to attach a video camera to a computer, thus adding visual capability to conversations. Ken Yamada, *Voice, Video Continue To Move To Web*, COMPUTER RESELLER NEWS, Dec. 2, 1996, at 1-2; see, e.g., *Video Conferencing on the Internet* (visited October, 21, 1996) <<http://141.163.121.36/TeachingLearning/NetTeaching/vidconf.html>> (also on file with the *Fordham International Law Journal*) (providing list of resources about Internet video conferencing).

82. Shea *ex rel. American Reporter*, 930 F. Supp. at 928.

83. Moran, *supra* note 81, at D9. To communicate using Internet telephony, both users in a conversation must have computers with microphones and speakers and connect to the Internet. Somogyi, *supra* note 81, at 2. Both users must use the same In-

lephony, users may contact someone that they know or choose someone from a list of users who subscribe to an Internet telephony service.⁸⁴ Current technology allows no effective way of determining any characteristics of members of IRC or Internet telephony because users know other participants only by the names the participants choose upon entering the group.⁸⁵

3. Usenet

Usenet is different from real time communications in that users do not communicate directly with each other.⁸⁶ Users instead communicate through posting⁸⁷ messages to subject-specific sections of usenet, referred to as newsgroups.⁸⁸ Users can transmit and receive any type of content to and from the newsgroups.⁸⁹ Presently there are newsgroups covering more than twenty-five thousand subjects.⁹⁰ Each day, users transmit almost 100,000 postings to these newsgroups.⁹¹ Once users post messages to newsgroups, anyone with access to usenet can view the messages.⁹²

4. FTP

FTP enables users to send files from one computer to another on the Internet.⁹³ Users providing content through FTP

ternet telephony software because different Internet telephony software programs do not necessarily interoperate. *Id.*

84. Joseph Szadkowski, *FreeTel Phones Home with No-Cost Sample*, WASH. TIMES, Dec. 2, 1996, at D9; *Freetel, Talk Over the Internet for Free* (visited Sept. 24, 1996) <<http://www.freetel.com>> (also on file with the *Fordham International Law Journal*).

85. *Shea ex rel. American Reporter*, 930 F. Supp. at 928 (noting that users can mask their identity by using pseudonym or giving fallacious details about their identity).

86. *See* Dern, *supra* note 29, at 196 (defining Usenet as series of networks on Internet where users can place messages).

87. *See* Dennis, *supra* note 2, at 586 (defining posting as sending content to Usenet).

88. *See* Dern, *supra* note 29, at 196 (defining newsgroups as places on Usenet where users post messages).

89. Henry H. Perritt, Jr., *Why Should Practicing Lawyers Be Interested in the Internet*, 443 PLI/PAT 47, 53-54 (1996).

90. Mike Boon et al., *Graffiti*, CALGARY HERALD, Nov. 15, 1996, at B14. *But see American Civil Liberties Union*, 929 F. Supp. at 835 (finding that there are 15,000 newsgroups). Newsgroups' addresses contain an indication of the type of content the newsgroup contains, such as "Comp" for computers, "Sci" for science, and "Alt" for alternative. Boon, *supra*, at 4.

91. *American Civil Liberties Union*, 929 F. Supp. at 835.

92. *Shea ex rel. American Reporter*, 930 F. Supp. at 928.

93. *It Helps to Know Internet Language*, PATRIOT-NEWS, Dec. 1, 1996, at D3. The word

can require a password for access.⁹⁴ Content providers⁹⁵ using FTP who allow anyone to access the content have no way of knowing who will gain access to that content.⁹⁶

5. The WWW

The WWW is the most widely used interactive Internet technology.⁹⁷ Like other content exchange technologies, the WWW is not separate from the Internet, but works on the Internet.⁹⁸ The WWW, like FTP, enables users to transfer files from remote computers to their own local computers.⁹⁹ Unlike FTP, however, the WWW uses a different protocol, http, which allows users to incorporate hyperlinks, graphics, and audio into web pages.¹⁰⁰

C. Undesirable Content

Governments disagree over the definition of undesirable content.¹⁰¹ Many governments find some degree of sexually explicit content undesirable.¹⁰² What may be illegal and thus, un-

"transfer" in file transfer protocol is misleading. Dern, *supra* note 29, at 271. FTP is the protocol users use to communicate. *Id.* at 275. FTP does not actually transfer a file from one computer to another. *Id.* at 271. FTP copies the file and sends the copy to the second computer. *Id.*

94. Dern, *supra* note 29, at 276.

95. See Volokh, *supra* note 50, at 2062 (referring to those providing content for Internet as "content providers.").

96. Shea *ex rel. American Reporter*, 930 F. Supp. at 928.

97. See Shipley & Fish, *supra* note 2, at 115 ("There is little doubt that the [WWW] is the fastest growing sector of the technology market."). *Id.*

98. *Id.* at 115.

99. Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 116 n.34 (1996).

100. Robert Grey, *Untangling the Web*, MARKETING, Dec. 1, 1996, at 25; see *supra* note 52 and accompanying text (discussing http).

101. See Commission Communication, *supra* note 13, COM (96) 487, at 11 (noting that definition of harmful content depends on cultural differences).

102. See Green Paper, *supra* note 15, COM (96) 483 Final at 15 (noting that although EU Member States have different standards on what type of sexually explicit content is legal, EU Member States universally ban child pornography in form of photos, photo-simulations, and animated material). The definition of child pornography varies between Member States. *Id.* Some Member States define and regulate child pornography with specific legislation, including Austria, Belgium, Denmark, the Netherlands, and the United Kingdom, and others by general obscenity rules, including Luxembourg, Portugal, and Spain. *Id.* at 37. Since September 1996, when Belgium experienced a pedophilia and mass murder scandal, European media has increased its focus on sexually explicit content. Suzanne Perry, *EU to Act Against Internet Child Exploitation*, REUTERS N. AM. WIRE, Sept. 27, 1996, available in LEXIS, News Library, Curnws File. It is difficult to determine exactly how much sexually explicit content is on

desirable in one country, may not be illegal in another country.¹⁰³ Governments might also find undesirable other types of content, including content that threatens national security,¹⁰⁴ human dignity,¹⁰⁵ minors,¹⁰⁶ and economic security.¹⁰⁷

D. *Shielding Users From Undesirable Internet Content*

Blocking access to undesirable content is a two-step process.¹⁰⁸ First one must determine that an Internet address contains such content.¹⁰⁹ Then one must prevent access to the content.¹¹⁰

I. Methods of Discerning Whether Internet Addresses Contain Undesirable Content and Whether Internet Content is undesirable

A user can discern if an Internet address contains undesirable content in various ways.¹¹¹ Users may employ a word and character search¹¹² which determines if content is undesirable based on the words or characters that comprise the content's

the Internet, but a U.S. Federal court has held that there is no evidence that sexually explicit content constitutes a substantial, or even significant, portion of the content available on the Internet. *Shea ex rel. American Reporter*, 930 F. Supp. at 931.

103. *Shea ex rel. American Reporter*, 930 F. Supp. at 931.

104. *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 such publications as Los Angeles Times, Washington Post, New York Times, and Wall Street Journal as threat to national security).

105. *CompuServe May Quit Germany Over Censorship Bill*, COMPUTERGRAM INT'L, Nov. 19, 1996, at 2 (relating German Government's desire to ban content demeaning to human dignity such as child pornography and neo-Nazi content).

106. *Reduced Bail Denied in Internet Sex Case South Whitehall*, ALLENTOWN MORNING CALL, Oct. 16, 1996, at B03. Some users have corresponded with children on the Internet in order to lure them into sexual encounters. *Id.* The California Police, for example, recently arrested a man for using the Internet to seek a sexual encounter with a 12-year-old boy. *Id.*

107. *See East Asian Censors*, *supra* note 104, at 19 (discussing undesirable content in Burma and Burma's prohibition on sending or receiving information on such topics as state security, economy, and national culture).

108. *See Danesh*, *supra* note 18, at 2.

109. *Id.*

110. *Id.*

111. *Shea ex rel. American Reporter*, 930 F. Supp. at 932.

112. *See id.* (discussing word and character search). A user may conduct a word and character search to search for characters or words that comprise an Internet address to determine if an address contains sexually explicit content. *Id.* Parents use software based on this method to protect their children. *Id.* Addresses, however, do not always contain words or characters signifying their content. *Id.*

address.¹¹³ The content provider may prompt¹¹⁴ the user, informing the user of the type of content contained at that address.¹¹⁵ An Internet address may also contain a rating,¹¹⁶ indicating the type of content at that address.¹¹⁷

a. Word and Character Search

One method of discerning whether an Internet address contains undesirable content is by looking to the words or characters that make up the Internet address and using those words or characters as an indicator of what type of content the Internet address contains.¹¹⁸ One Internet address, for example, is www.sex.com.¹¹⁹ The word "sex" in that address may indicate that the address contains sexually explicit content.¹²⁰ Users can configure the software they use to access the Internet to prevent access to addresses with objectionable words or phrases.¹²¹

b. Prompting

Users can also discern whether an Internet address contains undesirable content if content providers prompt users.¹²² Present technology enables a server to inform users of the type of content contained on a particular address or to query users for

113. *Id.*

114. *American Civil Liberties Union*, 929 F. Supp. at 845. When users attempt to retrieve content from a web page, the operator of the web page can prompt the user for information as a prerequisite for access. *Id.*

115. *Shea ex rel. American Reporter*, 930 F. Supp. at 932.

116. *See Danesh, supra* note 18, at 2 (defining rating as labeling content based on any number of criteria).

117. *See id.* (defining rating and providing examples of rating).

118. *See Shea ex rel. American Reporter*, 930 F. Supp. at 932 (detailing use of word and character search).

119. *Sex* (last visited Oct. 22, 1996) <<http://www.sex.com>> (also on file with the *Fordham International Law Journal*).

120. *See Shea ex rel. American Reporter*, 930 F. Supp. at 932 (noting that word "sex" or characters "xxx" might indicate sexually explicit content). In 1996, the America Online ban of the use of the word "breast" was met with protests from breast-cancer survivors. Edwin Diamond, *Censorship in Cyberspace*, *PLAYBOY*, June, 1996, at 70; *see* Clint Swett Bee, *America Offline: Throngs Of Users Join AOL — And Get Busy Signals*, *SACRAMENTO BEE*, Jan. 15, 1997, at D1 (noting that America Online provides both access to Internet and its own proprietary content for fee). In 1996, the White House's web page referred to the President's family as the first couple. *Id.* Some software prevented access to the web page because "couples" was a trigger word for that software. *Id.*

121. *Shea ex rel. American Reporter*, 930 F. Supp. at 932.

122. *Id.*

information before granting them access to web pages.¹²³ Based on this information, servers can then grant or deny access to a particular web page or a series of web pages.¹²⁴ Technologies other than the WWW do not have the ability to prompt and grant access.¹²⁵

c. PICS Based Rating

Rating is a process of labeling content as a shorthand to describe the content.¹²⁶ Content providers and third parties can rate either an Internet address or an Internet address' content, indicating the content type.¹²⁷ One expert has suggested rating content by inserting "-L18"¹²⁸ into an Internet address to indicate that the site is not suitable for individuals under the age of eighteen years old.¹²⁹

The WC3 developed PICS consists of technical specifications that provide Internet standards for rating formats.¹³⁰ Prior to PICS's implementation, there was no standard for labeling.¹³¹ PICS is analogous to specifying the place on a package that a label should appear and the size of the label, without specifying

123. *American Civil Liberties Union*, 929 F. Supp. at 845. Although technology is available, not all available software is capable of responding to such prompts by a web page. *Id.* at 845-46. Some large on-line service providers, for example, such as America Online and CompuServe, do not use software capable of responding to web page prompts. *Id.*

124. *See Shea ex rel. American Reporter*, 930 F. Supp. at 933-34 (discussing process of web pages granting or denying access). Content providers could prompt users for a credit card or some type of an adult identification code before allowing access to web pages. *American Civil Liberties Union*, 929 F. Supp. at 847 (noting that cost to web page providers in designing and maintaining adult access code screening systems and cost of using third party verification services, which do not charge web page providers to register their web pages, but charge users instead, may be prohibitive).

125. *American Civil Liberties Union*, 929 F. Supp. at 845-46.

126. *See Let the Market Flex its Muscle Over "Art"*, GREENSBORO NEWS & RECORD, NOV. 19, 1996, at A7 [hereinafter *Let the Market*] (defining rating as labeling).

127. *Shea ex rel. American Reporter*, 930 F. Supp. at 932; PICS, *Frequently Asked Questions*, (last modified Sept. 14, 1996) <<http://www.w3.org/pub/WWW/PICS/#FAQ>> (also on file with the *Fordham International Law Journal*) [hereinafter *Frequently Asked Questions*].

128. *Shea ex rel. American Reporter*, 930 F. Supp. at 932-33.

129. *Decision of the Day: Constitutional Law Computer Indecency Law Declared Void*, N.Y.L.J., Aug. 19, 1996, at 32.

130. Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, COMM. ACM, Oct. 1, 1996, at 87.

131. *Id.*

what the label should say.¹³² What the European Commission refers to as a wide coalition¹³³ supports PICS as a standard for rating content, including hardware and software manufacturers, ISPs, publishers, and content providers.¹³⁴

PICS can work with any Internet content exchange technology that has an address based on the uniform resource locator¹³⁵ ("URL") technology, including the WWW, FTP, and Usenet.¹³⁶ W3C has proposed a URL naming system for IRC which would enable PICS to work with these technologies.¹³⁷ The only Internet content exchange technology that PICS cannot work with is e-mail.¹³⁸ Software that recognizes ratings based on PICS is currently available.¹³⁹

Content providers and third party rating services can rate Internet content.¹⁴⁰ The content provider places his or her rating of the content in the content's address.¹⁴¹ One or more third party rating services can also rate the content without the

132. *Id.* at 2.

133. See Commission Communication, *supra* note 13, COM (96) 487, at 21-23 (detailing recommendations).

134. *Id.*

135. *Shea ex rel. American Reporter*, 930 F. Supp. at 933; see EDUCATOR'S GUIDE, *supra* note 74, at 219 (defining URL as address structure for WWW that other technologies can also use).

136. *American Civil Liberties Union*, 929 F. Supp. at 838; *Shea ex rel. American Reporter*, 930 F. Supp. at 932; *Frequently Asked Questions*, *supra* note 127.

137. Resnick & Miller, *supra* note 130, at 87; *Frequently Asked Questions*, *supra* note 127.

138. Resnick & Miller, *supra* note 130, at 87; *Shea ex rel. American Reporter*, 930 F. Supp. at 932; see *Frequently Asked Questions*, *supra* note 127 (discussing technologies that will and will not work with PICS technology).

139. *Shea ex rel. American Reporter*, 930 F. Supp. at 932; *American Civil Liberties Union*, 929 F. Supp. at 839. Microsoft's Internet Explorer 3.0, one of the leading software packages for using the Internet, is not only PICS-compatible, but also is free of charge. *Shea ex rel. American Reporter*, 930 F. Supp. at 932. This software allows parents to specify appropriate levels of violence or nudity at rated sites and view and block access to all unrated Internet sites. *Id.*

140. *Shea ex rel. American Reporter*, 930 F. Supp. at 932; see *PICS Rating Services*, PICS (last visited March, 12, 1997) <<http://www.classify.org/pics.htm>> (also on file with the *Fordham International Law Journal*) (listing links to several rating services providing different ways to categorize content).

141. *DTI: Ian Taylor Challenges Internet Service Providers—"Develop New Software to Come Clean"*, PRESSWIRE, Aug. 16, 1996, available in WESTLAW, Allnewsplus Database. The content provider first connects to a self-labeling service and describes the content to the service by filling out an on-line questionnaire. *Frequently Asked Questions*, *supra* note 127. The Internet content provider places a PICS compatible tag that the service provides in the address of the content. *Id.*

consent of the content provider.¹⁴² Third parties place their ratings of particular content on a separate server that PICS refers to as a label bureau.¹⁴³ The same content may receive different ratings from different third parties.¹⁴⁴ Parents or countries can choose a rating service whose judgments are based on values close to their own.¹⁴⁵ Individual countries can also act as their own rating service.¹⁴⁶

To block access to undesirable content, a user first indicates to the PICS compatible software a list of the categories of content that the user considers undesirable.¹⁴⁷ When a user tries to access content at a particular site, the user's software will check the ratings of the content against the list of undesirable categories.¹⁴⁸ The software can check the content provider's rating and the ratings of a particular third party, multiple third parties, or no third party.¹⁴⁹ If the content's ratings match the user's list of categories to exclude, the software will prohibit access.¹⁵⁰ The software can also limit users' access only to rated content.¹⁵¹

2. Methods of Shielding Users from Undesirable Content On the Internet

To shield users from undesirable content on the Internet, censors¹⁵² can prevent the transmitting of undesirable content

142. Terry Shannon, *News Briefs: Platform For Internet Content Selection (PICS)*, DATA-TRENDS REPORT ON DEC, Mar. 1, 1996, at 2; *Frequently Asked Questions*, *supra* note 127.

143. Resnick & Miller, *supra* note 130, at 87; *Frequently Asked Questions*, *supra* note 127.

144. Resnick & Miller, *supra* note 130, at 87; W3C, *PICS Statement of Principles* (visited Sept. 19, 1996) <<http://www.bilkent.edu.tr/pub/WWW/PICS/principles.html>> (also on file with the *Fordham International Law Journal*).

145. Danesh, *supra* note 18, at 2; *Frequently Asked Questions*, *supra* note 127. The PICS web page provides a list of rating services. W3C, *PICS Self-Rating Services* (last modified Sept. 14, 1996) <<http://www.w3.org/pub/WWW/PICS/selfrat.htm>> (also on file with the *Fordham International Law Journal*).

146. *Shea ex rel. American Reporter*, 930 F. Supp. at 932; see *Frequently Asked Questions*, *supra* note 127 (discussing how countries could use PICS).

147. Irwin Arieff, *Rating System Unveiled to Help Cull Unsavory Internet Material*, SAN DIEGO UNION TRIB., May 14, 1996, at 15; *Frequently Asked Questions*, *supra* note 127.

148. Herb Brody, *Toward a Cleaner, Tidier Net*, TECH. REV., Jan., 1996, at 11; *Frequently Asked Questions*, *supra* note 127.

149. *Sidebar*, DIGITAL KIDS REP., Mar. 1, 1996 at 2; *Frequently Asked Questions*, *supra* note 127.

150. Brody, *supra* note 148, at 5; *Frequently Asked Questions*, *supra* note 127.

151. Commission Communication, *supra* note 13, COM (96) 487, at 22.

152. See BLACK'S LAW DICTIONARY 153 (6th ed. 1991) (defining censorship as "review of publications, movies, plays, and the like for the purpose of prohibiting the pub-

to the Internet.¹⁵³ Censors can remove undesirable content from the Internet.¹⁵⁴ Censors can also prevent users from retrieving undesirable content.¹⁵⁵

a. Preventing the Transmitting of Undesirable Content to the Internet

Censors can prevent the transmitting of undesirable content to the Internet by stalling content in transit.¹⁵⁶ They may then scan the content for key words or phrases, and view it for undesirable audio or visual displays.¹⁵⁷ The stall and scan approach delays the forwarding of content to the Internet.¹⁵⁸

b. Removing Undesirable Content from the Internet

Censors can shield users by forcing removal of undesirable content already placed on the Internet.¹⁵⁹ Censors, for example, may force the content providers responsible for placing undesirable content on the Internet to remove the content.¹⁶⁰ Countries can do so only for content providers located within their respective boundaries because countries have no direct control over content that users place on servers in other countries.¹⁶¹

lication, distribution, or production of material deemed objectionable as obscene, indecent, or immoral.”).

153. *Hole In Defense*, DOW JONES ASIAN EQUITIES REP., Sept. 10, 1996, available in WESTLAW, Allnewsplus Database [hereinafter *Hole In Defense*]. For a government to censor content before users place it on the Internet, the government must force the user to access the Internet via government computers. *Id.* The government could then decide whether or not to place the content on the Internet. *Id.*

154. See *Banned President Mitterand Book*, *supra* note 16, at 2 (noting French Government's actions in bringing about removal of banned French book from Internet).

155. See Commission Communication, *supra* note 13, COM (96) 487, at 19-21 (discussing ways of preventing users from retrieving undesirable content, including allowing access only to sites known not to have desirable content or not allowing access to sites known to have undesirable content).

156. See *Hole In Defense*, *supra* note 153 (discussing that in order to stall content in transit, government must force users to send content via government computers).

157. See Steven Mufson, *Chinese Protest Finds a Path on the Internet*, WASH. POST, Sept. 17, 1996, at A09 (noting that governments cannot completely censor Internet content before users place it on Internet if content is in some type of code).

158. *Id.* If users encrypt content the stall and scan approach cannot discern undesirable content. *Id.* To encrypt is to decipher or decode. *Id.*

159. *Banned President Mitterand Book*, *supra* note 16, at 2

160. *Id.*

161. Robert Uhlig, *Lords of the Net to Patrol Their Creation*, DAILY TELEGRAPH, Sept. 24, 1996, at 8 (relating that governments have no control over ISPs located abroad).

c. Preventing Retrieval of Undesirable Content

One way to prevent access to Internet addresses containing undesirable content is through whitelisting,¹⁶² which allows access only to Internet addresses that censors choose.¹⁶³ Another way is through blacklisting,¹⁶⁴ the blocking of users' access to Internet addresses¹⁶⁵ known to contain undesirable content.¹⁶⁶ A third method of preventing access is by using software that prevents access based on a word and character search,¹⁶⁷ prompting,¹⁶⁸ or rating.¹⁶⁹

A country can directly allow or deny access to Internet addresses through the use of governmental proxy servers.¹⁷⁰ A country can indirectly blacklist by mandating that ISPs not allow users to access Internet sites containing undesirable content.¹⁷¹ A country can indirectly whitelist by mandating that ISPs only allow users to access Internet sites containing desirable content.¹⁷² Individuals can prevent themselves or family members from accessing undesirable content by using software that blocks access based on ratings, character search techniques, or blacklisting.¹⁷³ Software based on the whitelisting technique enables a

162. See Commission Communication, *supra* note 13, COM (96) 487, at 20 (defining whitelisting as allowing access only to sites known not to have undesirable content).

163. *Id.*

164. See *id.* at 20 (defining blacklisting as act of blocking users access to Internet addresses known to contain undesirable content).

165. See *Hole In Defense*, *supra* note 153 (noting that blacklisting identifies offending sites not by content, but by addresses).

166. Commission Communication, *supra* note 13, COM (96) 487, at 20.

167. *Id.*; see *supra* note 112 and accompanying text (discussing use of word and character search).

168. Commission Communication, *supra* note 13, COM (96) 487, at 20; see *supra* note 114 and accompanying text (discussing prompting).

169. *Shea ex rel. American Reporter*, 930 F. Supp. at 932.

170. See Michael Richardson, *Singapore Seeks to Assure Users on Internet Curbs*, INT'L HERALD TRIBUNE, Oct. 14, 1996, at 11, (noting that proxy servers are computers that screen all requests made by users and block access to banned sites); Joshua Gordon, *Cyber-Censorship Grows in East Asia*, L.A. TIMES, Sept. 27, 1996, at B9 (relating Singapore forcing its ISPs to route their users through governmental proxy servers).

171. See Minson, *supra* note 16, at 2 (discussing U.K. police hinting at arrests if ISPs did not prevent access to newsgroups containing illegal content).

172. Commission Communication, *supra* note 13, COM (96) 487, at 20; see *supra* note 162 and accompanying text (discussing whitelisting)

173. *American Civil Liberties Union*, 929 F. Supp. at 840-41 (explaining that individuals block access to Internet addresses by using software that first consults list of known addresses that contain undesirable content and then blocks access to addresses according to criteria chosen by individuals).

user to block all sites except for those that the user specifically chooses to make available.¹⁷⁴

E. European Union

In 1993, the Treaty of European Union created the European Union.¹⁷⁵ The European Union strives for economic integration through the creation of a common market¹⁷⁶ with four freedoms: the free movement of goods, services, persons, and capital.¹⁷⁷ The European Union also guarantees the right to freedom of expression.¹⁷⁸

1. Establishment of European Union

Concern over the use of steel and coal resources eventually led to the establishment of the European Union.¹⁷⁹ Following World War II, the United States and the United Kingdom called for the rearming of Germany as a buffer against Soviet expansion, while France cautioned against doing so.¹⁸⁰ Because the coal and steel industries were integral parts of both economic and military rebuilding, the 1951 Treaty of Paris created the European Coal and Steel Community¹⁸¹ ("ECSC"), which regulated the production of coal and steel as a compromise position all

174. *Shea ex rel. American Reporter*, 930 F. Supp. at 932; *American Civil Liberties Union*, 929 F. Supp. at 840-41.

175. TEU, *supra* note 11, art. G., O.J. C 224/1, at 5 [1992] 1 C.M.L.R. at 728.

176. *See* EC Treaty, *supra* note 12, art. 2, [1992] 1 C.M.L.R. at 588 (noting that Community shall "[establish] a common market" and asserting that common market provides principal medium to achieve Community functions).

177. *See id.*, art. 3, [1992] 1 C.M.L.R. at 588 (providing that activities of European Community shall include "an internal market characterized by the abolition, as between Member States, of obstacles to the free movement of goods, persons, services, and capital.").

178. *Id.*; *see supra* note 22, and accompanying text (detailing EU freedom of expression).

179. GEORGE A. BERMAN ET AL., *CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW* 5 (1993) (noting that France's fear of German use of coal and steel resources led to formation of European Union).

180. *Id.*

181. Treaty Establishing the European Coal and Steel Community, Apr. 18, 1951, 261 U.N.T.S. 140 [hereinafter ECSC Treaty], *as amended in* TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES (EC Off'l Pub. Off. 1987). The ECSC Treaty regulated coal and steel production. *See id.* art. 2, 261 U.N.T.S. 145 (establishing goal of creating common market to optimize productivity). The ECSC Treaty also promoted free trade within the participating countries. *See id.* art. 4(a), 261 U.N.T.S. at 147 (disallowing government quantitative restrictions and duties on imports and exports).

parties could accept.¹⁸² The Treaty of Paris signatories included France Germany, Belgium, Italy, Luxembourg, and the Netherlands.¹⁸³ In 1957, these six countries signed the Treaty of Rome,¹⁸⁴ establishing the European Economic Community ("EEC").¹⁸⁵ In 1993, the Treaty of European Union replaced the term European Economic Community with the term European Community.¹⁸⁶ The European Union Member States now include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Spain, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Sweden, and the United Kingdom.¹⁸⁷

2. The Common Market and the Four Freedoms

The EC Treaty envisages economic integration through the creation of a common market¹⁸⁸ with four freedoms, the free movement of goods, services, persons, and capital.¹⁸⁹ The free movement of goods requires removal of impediments to the free flow of goods in Member States, including elimination of Member States' customs duties and internal taxes.¹⁹⁰ The free movement of services includes the right of any national to travel

182. BERMANN ET AL., *supra* note 179, at 5. France originally proposed the Schuman plan, which eventually became the ECSC, named after France's foreign minister. *Id.* The Schuman plan placed all of Franco-German steel and coal production under a single authority, the High Authority, and allowed other countries to participate. *Id.* The High Authority would make decisions for the participating countries without their agreement. *Id.*

183. BERMANN ET AL., *supra* note 179, at 7.

184. EEC Treaty, *supra* note 11, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1 (providing term "Treaty of Rome").

185. Roger J. Goebel, *The European Union Grows: The Constitutional Impact of the Accession of Austria, Finland and Sweden*, 18 *FORDHAM INT'L L.J.* 1092, 1094 (1995). Due to fears that the French might reject the EEC, the six countries agreed on a second treaty, the Treaty Establishing the European Atomic Energy Community, which the French supported. BERMANN ET AL., *supra* note 179, at 7.

186. TEU, *supra* note 11, art. G., O.J. C 224/1, at 5 [1992] 1 C.M.L.R. at 728.

187. *See id.*, pmb., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725-26 (noting that until 1995, twelve EU Member States were Belgium, Denmark, France, Germany, Greece, Spain, Ireland, Italy, Luxembourg, Netherlands, Portugal, and United Kingdom).

188. *See* EC Treaty, *supra* note 12, art. 2, [1992] 1 C.M.L.R. at 588 (asserting that European Community shall establish common market and that common market provides principal medium to achieve Community functions).

189. *See id.*, art. 3, [1992] 1 C.M.L.R. at 588 (providing that activities of European Community shall include "an internal market characterized by the abolition, as between Member States, of obstacles to the free movement of goods, persons, services, and capital.").

190. *See id.*, arts. 9-37, [1992] 1 C.M.L.R. at 594-606 (detailing requirements of free

within the Member States to receive services,¹⁹¹ while the free movement of persons gives workers the right to accept employment in any Member State.¹⁹² Free movement of capital entails a prohibition on placing restrictions on the movement of capital.¹⁹³

3. Freedom of Expression

The European Union guarantees freedom of expression.¹⁹⁴ Member States also provide for freedom of expression in their respective constitutions.¹⁹⁵ The exercise of this right is subject to limitations for certain reasons, including the protection of health or morals and the prevention of crime.¹⁹⁶ Concern with the protection of minors has led to a limitation on freedom of expression through media regulation in the European Union.¹⁹⁷

movement of goods between Member States); BERMANN ET AL., *supra* note 179, at 317 (describing free movement of goods as "the key concept" among four freedoms).

191. See Council Directive 64/220, 56 J.O. L 845 (1964), O.J. Eng. Spec. Ed. 1963-1964, at 115, *corrected version in* Council Directive 73/148, O.J. L 172/14 (1973) (noting that right to receive services in any Member State comes from freedom to provide services); *Cowan v. Le Tresor Public*, Case 186/87, [1989] E.C.R. 195, [1990] 2 C.M.L.R. 613 (discussing that free movement of service's role is separate from that of other three fundamental freedoms).

192. EEC Treaty, *supra* note 11, 298 U.N.T.S. 11, 1973 Gr. Brit. T.S. No. 1.

193. TEU, *supra* note 11, pmb., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725-26; see *Public Prosecutor v. Guerrino*, Case 203/80, [1980] E.C.R. 2595 (noting that in practice free movement of capital is "a pre-condition for the effective exercise of other freedoms guaranteed by the Treaty."); BERMANN ET AL., *supra* note 179, at 606 (noting that free movement of capital is "a vital accessory to other three basic freedoms," in that, for example, "free movement of goods is impeded if payment for the goods is impeded.").

194. See Green Paper, *supra* note 15, COM (96) 483 Final at 32 (providing legal background on freedom of expression in European Union); *supra* note 22 and accompanying text (discussing EU freedom of expression).

195. See BERMANN ET AL., *supra* note 179, at 33 (charting each Member State's constitutional provisions for freedom of expression).

196. TEU, *supra* note 11, pmb., O.J. C 224/1, at 2 (1992), [1992] 1 C.M.L.R. at 725-26.

197. See Green Paper, *supra* note 15, COM (96) 483 Final at 6 ("stating the protection of minors and human dignity has always been a fundamental concern of media regulation."). Although Member States vary in their approaches to protection of minors through media regulation, the Commission notes that the measures required to enforce a total ban on illegal content are different from those needed to restrict access by minors or to prevent chance access by adults. *Id.*

II. COUNTRIES' ATTEMPTS AT REGULATING CONTENT ON THE INTERNET

Countries around the world are attempting to prevent undesirable Internet content from reaching their citizens.¹⁹⁸ The first country to take action against undesirable content on the Internet was an EU Member State, Germany.¹⁹⁹ Both EU Member States²⁰⁰ and non-EU Member States have since taken actions to combat undesirable Internet content.²⁰¹

A. European Union

EU Member States have made several attempts to regulate the Internet.²⁰² Among the Member States that have attempted such regulations are Germany, France, and the United Kingdom.²⁰³ In October 1996, the European Commission issued recommendations for a unified EU response to Internet regulation.²⁰⁴

1. Individual Member States

During the past two years, several EU Member States have tried to stop their citizens from accessing undesirable content on the Internet.²⁰⁵ In December 1995, German police requested that an ISP block the transmission of pornographic content on

198. See Amy Knoll, Comment, *Any Which Way But Loose: Nations Regulate the Internet*, 4 TUL. J. INT'L & COMP. L. 275, 276 (1996) (relating attempts at regulating Internet).

199. See *A Land of New Media Apathy*, *supra* note 16, at 8 (discussing German and French attempts at regulating Internet).

200. See Knoll, *supra* note 198, at 275 (discussing attempts at regulating Internet by EU Member States, including Germany and France).

201. See James Kyng, *Electronic Undesirables: SE Asian States Are Divided on How to Police the Internet*, FIN. TIMES, Sept. 9, 1996, at 17 (noting Asian countries' attempts at regulating Internet); Sarah Gauch, *Web Becomes Arab Mini-Mecca: But It's Not Surf's Up for All*, CHRISTIAN SCI. MONITOR, July 9, 1996, at 1 (discussing views of Internet by such Middle Eastern governments as Egypt, Saudi Arabia, and Iran).

202. See *A Land of New Media Apathy*, *supra* note 16, at 8 (discussing attempts of German and French Governments at regulating Internet).

203. See *id.* (detailing German police request that CompuServe block access to newsgroups containing pornographic content).

204. See Commission Communication, *supra* note 13, COM (96) 487, at 21-24 (discussing recommendations).

205. See Wanchek, *supra* note 17 (discussing attempts at regulating Internet by several EU Member States, United States, and China).

the Internet.²⁰⁶ In January 1996, the French Government tried to remove a banned book from the Internet.²⁰⁷ The United Kingdom, concerned about pornographic Internet content, initiated plans in October 1996 to stop such content from reaching British citizens.²⁰⁸

a. Germany

The growth of the Internet in Germany has been slow.²⁰⁹ As of 1996, only two percent of German citizens report that they use the Internet at home or at work.²¹⁰ Seventy-eight percent reported that they had never heard of the Internet.²¹¹

In December 1995, Germany became the first EU Member State to attempt to regulate the Internet.²¹² German police requested that CompuServe,²¹³ an ISP, block the transmission of pornographic newsgroups²¹⁴ on the Internet.²¹⁵ CompuServe first responded by blocking access to 200 newsgroups having the word sex in their addresses, but later reinstated access, instead providing subscribers with software that allows users to independently prevent access to undesirable content.²¹⁶

206. See *A Land of New Media Apathy*, *supra* note 16, at 8 (noting German police request that CompuServe block transmission of pornographic newsgroups on Internet).

207. *Id.*; see *supra* note 154 and accompanying text (noting France's actions in removing banned French book from Internet).

208. See Uhlig, *supra* note 138, at 8 (detailing U.K. proposal for protecting its citizens from undesirable Internet content); 'Safety Net' on Internet Will Catch Child Porn, DAILY TELEGRAPH, Sept. 23, 1996, at 8 [hereinafter 'Safety Net' on Internet] (discussing plan to stop undesirable content from reaching U.K. citizens).

209. *A Land of New Media Apathy*, *supra* note 16, at 8.

210. *Id.*

211. *Id.*

212. See Kimberly A. Strassel, *Parents Are Given a Tool to Limit Internet Access*, WALL ST. J. EUR., Aug. 22, 1996, at 4 (discussing Germany's attempts at regulating Internet by requesting that CompuServe stop access to newsgroups containing sexually explicit content).

213. See Commission Communication, *supra* note 13, COM (96) 487, at 15 n.11 (noting that CompuServe is U.S. based company whose services include providing access to Internet); CompuServe, *Company Information* (last visited October 20, 1996) <<http://world.compuserve.com/world/corporate/index.html>> (also on file with the *Fordham International Law Journal*) (detailing CompuServe's company information).

214. See Dern, *supra* note 29, at 196 (defining newsgroups as place on Usenet where users place messages).

215. *It's a Filthy War*, SCOT. ON SUNDAY, Sept. 15, 1996, at 7. Although the German police contend that they requested CompuServe's compliance, CompuServe contends that German police demanded compliance. *Id.*

216. Edwin Diamond, *Censorship in Cyberspace*, PLAYBOY, June, 1996, at 70.

b. France

The French Government also has tried to block access to undesirable content.²¹⁷ In January 1996, the French Government took action against what it viewed as undesirable Internet content.²¹⁸ The Government banned a book,²¹⁹ which details France's President Francois Mitterand's alleged misrepresentations about his health.²²⁰ When this book appeared on a web page located on a server in France, the Government forced the ISP to remove the web page containing the book from the server.²²¹ The banned book's content, however, soon appeared on web pages located on servers outside of France, allowing all users, including French users, to access the content.²²² As the servers containing the content resided outside of France, the French Government could not force the removal of the content from the servers.²²³

c. United Kingdom

The U.K. Government is concerned about the amount of child pornography²²⁴ on the Internet.²²⁵ In an attempt to stop U.K. citizens from accessing illegal content, the police, in August 1996, sent a letter to ISPs identifying 133 newsgroups that the ISPs were transmitting to their subscribers and that the police believed to be illegal.²²⁶ The police wanted the ISPs to regulate themselves and alluded to the possibility of arrests if the ISPs

217. See Wanchek, *supra* note 17 (detailing France's attempts at regulating Internet).

218. Dern, *supra* note 29, at 196.

219. *Banned President Mitterand Book*, *supra* note 16, at 2. The French Government banned the book, *Le Grand Secret*, in January 1996 because the Mitterand family claimed the book constituted a breach of doctor-patient confidentiality. *Id.*

220. L.T. Greenberg, *Is Big Brother Hanging by His Bootstraps? National Governments and Information Technologies*, COMM. OF THE ACM, July, 1996, at 11.

221. Dern, *supra* note 29, at 196.

222. *A Land of New Media Apathy*, *supra* note 16, at 8; Greenberg, *supra* note 220, at 11.

223. See Uhlig, *supra* note 138, at 8 (noting that governments have no control over ISPs located abroad).

224. Thomas Sanction, *Preying on the Young*, TIME (international edition), Sept. 2, 1996, at 22. Possession of child pornography is legal in Mexico, Sweden, Japan, and Hungary. *Id.* In Belgium, publication of child pornography carries a maximum sentence of one year. *Id.*

225. 'Safety Net' on Internet, *supra* note 208, at 8.

226. See Sharon Smith, *To Protect or Serve?*, COMPUTER WKLY, Oct. 3, 1996, at 36 (discussing legal and social ramifications of letter that police sent to ISPs); Andrew

failed to do so.²²⁷

After the police warning, Pipex, the largest U.K. ISP, put forth proposals for preventing undesirable content from reaching U.K. citizens.²²⁸ The result was that Safety-Net, which began operation in October 1996, now enjoys the backing of the trade organizations that represent U.K. ISPs.²²⁹ Safety-Net, which Pipex funded,²³⁰ set up telephone, fax, and e-mail hotlines to allow users to notify it of illegal content on the Internet.²³¹ Safety-Net then informs British ISPs about the identified illegal content to which the ISPs can then block access.²³²

2. European Union

In October 1996, the Commission recommended action for combating illegal²³³ and harmful²³⁴ content on the Internet.²³⁵ For illegal content on the Internet, the Commission recommended stronger cooperation between Member States in combating the sources of illegal content and in restricting copying of it to other places on the Internet.²³⁶ The Commission also called for a clarification on the liability of ISPs²³⁷ and en-

Brown, *The Net Effect is Confusion*, INDEPENDENT, Sept. 24, 1996, at 2 (noting letter police sent to ISPs).

227. Minson, *supra* note 16, at 2.

228. *British Gov't Moves To Stamp Out Internet Porn*, NEWSBYTES, Sept. 27, 1996, at 1 [hereinafter *British Gov't Moves*].

229. 'Safety Net' on Internet, *supra* note 208, at 8 (noting that trade organizations that represent U.K. ISPs, including Internet Service Providers' Association and London Internet Exchange support Safety-Net).

230. *British Gov't Moves*, *supra* note 228, at 2.

231. Uhlig, *supra* note 138, at 8.

232. 'Safety Net' on Internet, *supra* note 208, at 8.

233. See Commission Communication, *supra* note 13, COM (96) 487, at 10 (noting that "the Internet does not exist in a legal vacuum, since all those involved . . . are subject to the respective laws of the Member States."). "It is a matter for Member States to define what is illegal by law and to enforce it by detecting illegal activity and punishing offenders." *Id.* at 11.

234. See *id.* at 3(b) (discussing that definition of harmful content depends on cultural differences and that "each country may reach its own conclusion in defining borderlines between what is permissible and not permissible.").

235. Dern, *supra* note 29, at 196.

236. See Commission Communication, *supra* note 13, COM (96) 487, at 24-25 (calling for cooperation in exchange of "information on those providing criminal content and [enforcing] existing laws relating to criminal material," and encouraging "Member States to define minimum European standards on criminal content.").

237. See *id.* at 25 (pointing out "the need for a common European framework to clarify administrative rules and regulations which apply to access providers and host service providers should be assessed.").

couraged ISP self-regulation.²³⁸ For harmful content, the Commission recommended that content providers and rating services²³⁹ rate content based on PICS,²⁴⁰ and that users employ software to block access to undesirable content based on PICS ratings.²⁴¹ The Commission also calls for an extension of the dialogue on the best way to control harmful and illegal Internet content to include the largest number of countries possible.²⁴²

B. Other Countries

Many non-EU Member States are also grappling with the best way to regulate the Internet.²⁴³ The U.S. Congress enacted legislation to protect minors from exposure to undesirable content on the Internet.²⁴⁴ Asian countries, notably Singapore and China, have also been trying to stop their citizens from accessing objectionable Internet content.²⁴⁵ Israel and Arab countries are

238. *See id.* at 13 (noting that self regulation has already started in United Kingdom with Safety-Net).

239. *See id.* at 23 (calling for setting up multiple EU rating services "to ensure that users have access to rating systems suitable to their needs, and in order to avoid a situation whereby they have to rely on rating systems developed for the US where there may be a different approach on what is suitable content for minors . . .").

240. *See id.* at 20 (positing that PICS enables "empowering [of] parents to protect minors.").

241. *See id.* at 25 (detailing need to encourage European content providers to cooperate in rating system by adopting their own code of conduct for content published on Internet and need to inform parents and teachers about rating system).

242. *See id.* at 26 ("positing [s]ince this dialogue must include the largest number of countries possible, it could be extended to a body with a larger membership such as the OECD, the World Trade Organization, the United Nations, or one of the more specialized United Nations bodies.").

243. *See Where Wizards Stay*, *supra* note 33, at 65 (detailing Internet regulations in several countries, including United States, China, and Singapore).

244. *See* 47 U.S.C. § 223(d)(1996) (laying out provisions of legislation to protect minors). The U.S. Government recognizes that the Internet offers opportunities for diverse political discourse and cultural development and opens many avenues for intellectual activity. 47 U.S.C. § 230(a)(3)(1996) (finding that Internet offers "forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."). Several states, including Georgia and New York, have since passed measures regulating Internet. Art Kramer, *ACLU Sues the State Over its Ban on Some Internet Communication*, ATLANTA J. & CONST., Sept. 25, 1996, at 1. *See* Rose Aguilar, *50 Ways to Go to Jail*, CNET NEWS, Sept. 14, 1996 <<http://www.news.com/SpecialFeatures/0,5,3449,00.html>> (also on file with the *Fordham International Law Journal*) (discussing legislation in United States regulating Internet).

245. *See* Kynge, *supra* note 201, at 17 (discussing Asian countries' attempts at regulating Internet).

grappling with how best to use the Internet.²⁴⁶

1. United States

In February 1996, in an effort to protect minors from sexually explicit content, the U.S. Congress enacted the Communications Decency Act of 1996 ("CDA").²⁴⁷ Section 223(d) of the CDA²⁴⁸ makes it a crime to use the Internet to transmit or display patently offensive sexual or excretory activities or sexual organs to persons under the age of eighteen.²⁴⁹ The criminal penalty for violating § 223(d) is a fine up to US\$250,000, imprisonment of not more than two years, or both.²⁵⁰

The CDA also provides two "safe harbor"²⁵¹ affirmative defenses²⁵² to prosecution.²⁵³ The first defense applies to individuals who have taken reasonable and effective actions in good faith to restrict or prevent access by minors to CDA-prohibited communication.²⁵⁴ The CDA provides the second affirmative de-

246. See Gauch, *supra* note 201, at 1 (detailing views of Internet by Middle Eastern governments including Egypt, Saudi Arabia, and Iran).

247. See *supra* note 244 and accompanying text (relating U.S. Congress' motives in enacting Communications Decency Act of 1996 ("CDA")).

248. 47 U.S.C. § 223(d)(1996). The statute states:

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

Id.

249. 47 U.S.C. § 223 (1996). This section does not define the Internet. *Id.* Instead, it employs the term "interactive computer service." *Id.* Congress, however, has made it clear that the term "interactive computer service" includes "a service or system that provides access to the Internet." *Id.* at (e)(2).

250. *Id.* at (d).

251. See *American Civil Liberties Union*, 929 F. Supp. at 829 (describing affirmative defenses to CDA as "safe harbor defenses.").

252. See BLACK'S LAW DICTIONARY, *supra* note 152, at 38 (defining affirmative defense as "in pleading, matter asserted by defendant, which assuming the complaint to be true, constitutes a defense to it.").

253. See 47 U.S.C. § 223(e)(5)(1996) (setting out affirmative defenses).

254. *Id.*

fense to individuals who have restricted access to CDA prohibited communication by requiring use of some type of identification, including a credit card, debit account, adult access code, or adult personal identification number.²⁵⁵

Two district courts, one in the Southern District of Pennsylvania²⁵⁶ and the other in the Eastern District of New York,²⁵⁷ have since held the CDA to be unconstitutional.²⁵⁸ In *American Civil Liberties Union v. Reno*, The American Civil Liberties Union²⁵⁹ ("ACLU") filed a motion for a temporary restraining order²⁶⁰ ("TRO") against the CDA with the Pennsylvania district

It is a defense to a prosecution under the CDA that a person has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology

Id.

255. 47 U.S.C. § 223(e)(5)(B)(1996). It is a defense to a prosecution under the CDA that a person "has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number." *Id.* The CDA itself does not provide a definition of adult access code or adult personal identification number. *Id.* A user can gain an adult access code or adult personal identification code from a content provider. *American Civil Liberties Union*, 929 F. Supp. at 934. The code would serve as evidence of a user's age. *Id.* A user can also obtain a code from a third party service and use the code to retrieve content placed on the Internet by any content provider registered with the service. *Id.*

256. *American Civil Liberties Union*, 929 F. Supp. at 824.

257. *Shea ex rel. American Reporter*, 930 F. Supp. at 916.

258. *See id.* (holding CDA unconstitutional). The second district court found that nonmutual offensive collateral estoppel does not apply in this case and, thus, the first court's decision does not preclude this court from deciding the issues presented in its case. *Shea ex rel. American Reporter*, 930 F. Supp. at 924 n.1. President Bill Clinton has since ordered the Department of Justice to appeal the decisions. Nat Hentoff, *The Constitution Lost the Election*, ROCKY MTN. NEWS, Nov. 18, 1996, at 39A.

259. *American Civil Liberties Union*, 929 F. Supp. at 827. In addition to the American Civil Liberties Union, the plaintiffs included Human Rights Watch, Electronic Privacy Information Center, Electronic Frontier Foundation, Journalism Education Association, Computer Professionals for Social Responsibility, National Writers Union, Clarinet Communications Corp., Institute for Global Communications, Stop Prisoner Rape, AIDS Education Global Information System, Bibliobytes, Queer Resources Directory, Critical Path AIDS Project, Inc., Wildcat Press, Inc., Declan McCullagh dba Justice on Campus, Brock Meeks dba Cyberwire Dispatch, John Troyer dba The Safer Sex Page, Jonathan Wallace dba The Ethical Spectacle, and Planned Parenthood Federation of America, Inc. *Id.* at 827 n.2. The court refers to all plaintiffs collectively as the ACLU. *Id.*

260. *See BLACK'S LAW DICTIONARY*, *supra* note 152, at 1021. *Black's Law Dictionary* defines a temporary restraining order ("TRO") as:

[A]n emergency judicial remedy of brief duration which may issue only in exceptional circumstances and only until the trial court can hear arguments

court the day that the CDA took effect.²⁶¹ The district court granted the TRO, finding that the CDA was unconstitutionally vague.²⁶² In June 1996, the court granted the ACLU's motion for a preliminary injunction²⁶³ against the CDA, unanimously ruling that the CDA is unconstitutional in that it is substantially overbroad because it effectively forces many Internet users to refrain from constitutionally protected speech or risk criminal prosecution.²⁶⁴

or evidence, as the circumstances require, on the subject matter of the controversy and otherwise determine what relief is appropriate.

Id. See *Dunlow v. Ibara*, 82 F.3d 409, (4th Cir. 1996) (holding that because "no exceptional circumstances exist, the denial of Appellant's motion for a temporary restraining order is not appealable.").

261. *American Civil Liberties Union*, 929 F. Supp. at 827.

262. *Id.* at 849 (finding 47 U.S.C. § 223(a)(1)(B) of CDA unconstitutionally vague). 47 U.S.C. § 223(a)(1)(B) states that the Government shall fine, imprison for not more than two years, or both, whoever:

[B]y means of a telecommunications device knowingly (i) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication.

Id.

263. Fed.R.Civ. P. 65. The Federal Rules of Civil Procedure charges:

[A] preliminary injunction should be granted only upon a clear showing by party seeking the extraordinary remedy of (1) probable success upon a trial on the merits, and (2) likely irreparable injury to him unless the injunction is granted, or (3) if his showing of probable success is limited but he raised substantial and difficult issues meriting further inquiry, that the harm to him outweighs the injury to others if it is denied.

Id.

264. *American Civil Liberties Union*, 929 F. Supp. at 849 (stating "§§ 223(a)(1)(B) and 223(a)(2) of the CDA are unconstitutional on their face to the extent that they reach indecency."). § 223 (a) (2) states that whoever:

[K]nowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

47 U.S.C. § 223(a)(2) (1996). Judge William Sloviter, the Chief District Judge wrote:

There has been recent public interest in the female genital mutilation routinely practiced and officially condoned in some countries. News articles have been descriptive, and it is not stretching to assume that this is a subject that occupies news groups and chat rooms on the Internet. We have no assurance that these discussions, of obvious interest and relevance to older teenage girls, will not be viewed as patently offensive—even in context—in some communities.

American Civil Liberties Union, 929 F. Supp. at 853. Judge Brian Buckwalter, another Pennsylvania District Judge, wrote that he believes "that the word 'indecent' is unconsti-

In *American Reporter v. Reno*, The editor-in-chief and part owner of the American Reporter, a newspaper published exclusively on the Internet,²⁶⁵ brought the second cause of action regarding the CDA in the New York District Court. The American Reporter sought a declaration that the CDA was unconstitutionally overbroad and vague.²⁶⁶ In July 1996, the New York District Court ruled that the CDA was unconstitutional,²⁶⁷ holding that the CDA was overbroad in that it would serve as a ban on constitutionally protected, indecent communication between adults.²⁶⁸

2. Asian Countries

Asian countries are grappling with how to regulate the Internet.²⁶⁹ Singapore, in July 1996, began regulating the Internet through the use of proxy servers.²⁷⁰ The other members of the Association of Southeast Asian Nations²⁷¹ ("ASEAN") have not

tutionally vague, and [he] find[s] that the terms 'in context' and 'patently offensive' also are so vague as to violate the First and Fifth Amendments." *Id.* at 858. The other Pennsylvania District Judge, Judge George Dalzell, wrote, "I conclude that the disruptive effect of the CDA on Internet communication, as well as the CDA's broad reach into protected speech, not only render the CDA unconstitutional but also would render unconstitutional any regulation of protected speech on this new medium." *Id.* at 867.

265. *American Reporter*, 930 F. Supp. at 923-24.

266. *Id.* On February 8, 1996, following the signing of the CDA, the American Reporter published an editorial on the Internet criticizing Congress for the passage of the CDA. *Id.* The editorial contained language arguably falling within the scope of § 223(d). *Id.* After publishing the editorials, the American Reporter moved for preliminary injunctive relief to prevent the Department of Justice from enforcing the CDA. *Id.* at 924.

267. *See id.* at 923 ("[W]e reach the inescapable conclusion that § 223(d) will serve to chill protected speech."). The court added that not only was § 223(d) overbroad, but also the affirmative defenses set out in § 223(e)(5) cannot, with current technology, effectively protect adult content providers wishing to engage in constitutionally protected indecent communication. *Id.* The court, however, held that § 223(d) is not unconstitutionally vague. *Id.* "The definition of material regulated by [§ 223(d)] is a familiar one, repeatedly upheld against vagueness challenges in a line of jurisprudence concerning television and radio broadcasting, cable programming, and commercial telephone services." *Id.*

268. *Id.*

269. *See Gordon, supra note 170*, at B9 (discussing censorship of Internet by Asian countries including China and Singapore); MSNBC, *Governments Take on the Net* (visited Oct. 18, 1996) <<http://www.msnbc.com/news/30205.asp>> (also on file with the *Fordham International Law Journal*) (detailing China and Singapore's attempts at regulating Internet).

270. *Gordon, supra note 170*, at B9.

271. *Fact sheet: Association of Southeast Asian Nations. (includes information on Regional Forum members)*, U.S. DEP'T ST. DISPATCH, Vol. 6, No. 31, ISSN: 1051-7693. Indonesia, Malaysia, the Philippines, Singapore, and Thailand formed the Association of Southeast

taken significant action in regulating the Internet.²⁷² In September 1996, China followed Singapore's use of a proxy server and blocked access to one hundred WWW sites.²⁷³

a. Singapore

In July 1996, the Singapore Broadcasting Authority²⁷⁴ ("SBA"), the governmental agency that regulates broadcasting in Singapore, initiated Internet regulations to protect users, particularly the young, against the broadcast of unlawful or undesirable content.²⁷⁵ The SBA's regulations apply to ISPs²⁷⁶ and any users who provide content for business, political, or religious purposes on the WWW.²⁷⁷ The regulations require ISPs to obtain a license from the SBA to operate.²⁷⁸ While ISPs must block SBA-blacklisted sites,²⁷⁹ the SBA has not announced which sites

Asian Nations ("ASEAN") in 1967 to promote political and economic cooperation with member countries. *Id.* at 1. Brunei joined ASEAN in 1984, the same year Brunei gained its independence from the United Kingdom. *Id.* at 1-2. Vietnam joined in 1995. *Id.* at 2. ASEAN established the ASEAN Free Trade Area ("AFTA"), which initiated a process of eliminating the majority of tariffs on manufactured goods between the member countries. *Id.* ASEAN played a key role in the international efforts to terminate the conflict in Cambodia, which led to the democratic elections in Cambodia in 1993. *Id.*

272. See *ASEAN Agrees on Need for Regulation of Internet*, ASIAN ECON. NEWS, Sept. 9, 1996, available in WESTLAW, Allnewsplus Database [hereinafter *ASEAN Agrees*] (relating South East Asian countries' views on Internet).

273. *China Says Control of Internet Sites is 'Normal'*, DOW JONES BUS. NEWS, Sept. 12, 1996, at 6:07.

274. *Singapore Telecom Authority to Add New Member in Network*, DOW JONES ASIAN EQUITIES REP, Sept. 10, 1996, available in WESTLAW, Allnewsplus Database. The Singapore Government established the Singapore Broadcasting Authority ("SBA") as part of a consortium in charge of the Singapore ONE network, a computer network connecting Singapore's computers. *Id.* The other members of the consortium are the Telecommunication Authority of Singapore, the National Computer Board, and the National Science & Technology Board. *Id.* The SBA's role is to regulate content on the Singapore ONE network. *Id.*

275. Singapore Broadcasting Authority, *News Release*, Singapore Broadcasting Authority, at 3 (last modified July, 11, 1996) <<http://www.gov.sg/sba/netreg/regrel.htm>> (also on file with the *Fordham International Law Journal*) (stating that "[the regulatory scheme] encourages minimum standards in cyberspace and seeks to protect [Internet] users, particularly the young, against the broadcast of unlawful or objectionable materials.").

276. The Class License Scheme, annex A, § 2 (1996) (Sing.).

277. *Id.* § 11. "Individuals who put up [web pages] will be exempted from the class licence scheme, unless they are operating these web pages for business, political and religious purposes." *Id.*

278. *Id.* § 11.

279. *Id.* § 5. "The SBA recognises that it would be impossible to actively monitor

are on its blacklist, or even how many sites the blacklist contains.²⁸⁰ The SBA-regulations require ISPs to use their best efforts to avoid allowing access to content that harms public morals,²⁸¹ racial and religious harmony,²⁸² and security or national defense.²⁸³ The regulations also encourage, but do not mandate, ISP and parental use of software that guards against access to undesirable content.²⁸⁴

The Singapore Government is enforcing the SBA-regulations by using governmental proxy servers.²⁸⁵ The Government forces ISPs to route their users through Government computers that can deny access to sites on the Government blacklist.²⁸⁶ If an ISP does not follow the regulations, the SBA may cancel or suspend the ISP's license or require the ISP to pay a fine.²⁸⁷

The Government's use of proxy servers in Singapore led to several problems.²⁸⁸ The use of proxy servers increased the time necessary to access content on the Internet because the servers could not handle the amount of computer traffic.²⁸⁹ To alleviate the traffic, the SBA has since allowed most businesses to circumvent the proxy servers.²⁹⁰

the Internet to pre-censor objectionable sites. As such, ISPs will only be required to block out objectionable sites as directed by SBA." *Id.*

280. Tom Standage, *Connected: Web Access In a Tangle As Censors Have Their Say: Singapore Wants to Regulate What Is Broadcast On The Internet*, DAILY TELEGRAPH, Sept. 10, 1996, at 3.

281. The Class License Scheme, annex C, § 6 (1996) (Sing.). Content that harms public morals includes content that "propagates promiscuity, depicts gross exploitation of violence, nudity, sex, or horror," or depicts "sexual perversions such as homosexuality, lesbianism, or pedophilia." *Id.*

282. *Id.* § 5. Content is harmful to racial and religious harmony if it "denigrates any racial or religious group, brings any race or religion into resentment, or promotes religious deviations or occult practices such as Satanism." *Id.*

283. *Id.* § 4. Content that harms public security or national defense includes content that "undermines the public confidence in the government, or presents information or events in such a way that alarms or misleads any part of the public." *Id.*

284. *Id.*, annex A, § 7.

285. Gordon, *supra* note 170, at B9.

286. *Id.*

287. Singapore Broadcasting Authority, *Censorship and Free Speech*, (last modified Aug. 1996) <<http://www.gov.sg/sba/letter3.htm>> (also on file with the *Fordham International Law Journal*).

288. See Uhlig, *supra* note 138, at 8 (discussing problems with Singapore's proxy server).

289. *Id.* at 8.

290. See Jack Robertson, *Net Escape*, ELECTRONIC BUYERS' NEWS, Sept. 16, 1996, at 2 (noting that because of problems with proxy servers, Singapore Government allows most businesses to circumvent servers).

b. Other ASEAN Countries

Aside from Vietnam, none of the ASEAN countries have followed Singapore's lead in regulating the Internet.²⁹¹ The Malaysian Government²⁹² has pledged that there will be no Government-imposed censorship of Internet content.²⁹³ It is studying instead the idea of users policing themselves.²⁹⁴ Indonesia is also considering the idea of self-policing by users.²⁹⁵ The Philippines and Thailand advocate minimal government intervention with self-policing by ISPs.²⁹⁶

In May 1996, the Vietnamese Government announced regulations for the Internet.²⁹⁷ The regulations state that all ISPs must register with the Government and are subject to official inspections.²⁹⁸ The Government has pledged to shut down ISPs that allow access to content that is harmful to national interests.²⁹⁹

In September 1996, Singapore hosted a three-day ASEAN conference to formulate a common approach for addressing legal and social issues that use of the Internet raises.³⁰⁰ The ASEAN member nations could not agree on a common approach.³⁰¹ Instead, they issued a joint statement agreeing that the appropriate approach to Internet regulations should depend on the culture and legal system of each particular country.³⁰²

291. *KL Looking Into Ways to Censor Internet*, SINGAPORE STRAITS TIMES (Singapore), Sept. 23, 1996, at 23.

292. *See id.* (noting that although Malaysian Government recognizes economic benefits of Internet, it believes that Western culture and values dominate Internet, and could be threat to Malaysia's culture, values, and business systems).

293. Kynge, *supra* note 201, at 17.

294. *Id.*

295. *Id.*

296. *ASEAN Internet Forum Fails to Produce Common Strategy to Police the Net*, AGENCE FR.-PRESSE, Sept. 4, 1996, at 1.

297. *See Vietnam Regulations Part of Power Play for Internet*, NEWSBYTES, June 10, 1996, at 2 (relating internal Vietnamese politics leading to regulation of Internet). Presently, Vietnam only has the capability to send e-mail over the Internet. *Id.* at 4. Vietnam's connection to the Internet runs from the Institute for Information Technology in Hanoi to the Australian National University. *Id.* Researchers, scientists, and foreign residents are the main users of the Internet in Vietnam. *Id.*

298. *Id.* at 2.

299. *Vietnam Keeps Grip on Internet Access*, ROCKY MOUNTAIN NEWS, June 16, 1996, at 40A.

300. *See ASEAN Agrees*, *supra* note 272, at 3 (discussing AESAN conference).

301. Kynge, *supra* note 201, at 17.

302. *See id.* (noting that reluctance to regulate Internet is due to these countries

c. China

In June 1996, China sent a top official to study Singapore's approach to restricting access to the Internet.³⁰³ In September 1996, China blocked access to one hundred WWW sites, including major Western news media sites,³⁰⁴ sites that monitor human rights abuses,³⁰⁵ and sites containing sexually explicit content.³⁰⁶ The Chinese Government is enforcing its regulations by using government proxy servers,³⁰⁷ forcing ISPs to channel all users through Government computers which block access to banned sites.³⁰⁸

3. Israel

The Israeli Government does not regulate access to the Internet.³⁰⁹ It allows Palestinians to use its telephone lines to access the Internet.³¹⁰ Israel-based companies produce cutting-edge Internet related products.³¹¹

4. Arab Countries

Arab countries addressing the question of whether the Internet either presents an opportunity to help their economies or presents a source of negative foreign influences, have allowed

believing that Internet will play significant role in their commercial future); *ASEAN Agrees*, *supra* note 272, at 2 (relating events leading up to joint statement).

303. Sheila Tefft, *China Attempts to Have Its Net and Censor It Too*, *CHRISTIAN SCI. MONITOR*, Aug. 5, 1996 at 1.

304. *East Asian Censors*, *supra* note 104, at 19 (discussing that among blocked sites are Los Angeles Times, Washington Post, New York Times, Wall Street Journal, Amnesty International, and Human Rights Watch/Asia).

305. *Id.*

306. *See Hole In Defense*, *supra* note 153, at 2 (noting that China has blocked access to the web pages of Playboy and Penthouse).

307. *See Richardson*, *supra* note 170, at 11 (defining proxy server).

308. Gordon, *supra* note 170, at B9.

309. Winston Pickett, *Surfing the Internet*, *JERUSALEM POST*, June 28, 1995, at 5 (noting that in Israel, user only needs computer and modem to access Internet).

310. *Palestinians Accuse Israel of Blocking Internet Access*, *AGENCE FR.-PRESSE*, Oct. 7, 1996, at 8A.

311. *See Telephony*, *COMM. DAILY*, Mar. 11, 1996, at 1 (relating Israel-based company that plans to market software that enables telephone calls through Internet to telephones not connected to computers); *Windows Prgm Supports Multilingual Web Pages*, *NEWSBYTES*, June 15, 1995, at 1 (discussing Israeli-based company's software that enables users to access and author web pages using any language version of Microsoft Windows, computer operating system).

access to the Internet in varying degrees.³¹² The Saudi Arabian Government controls access to the Internet by having a single connection to the Internet³¹³ and provides limited Internet access to hospitals and universities.³¹⁴ In 1993, the Egyptian Government offered free access to the Internet to spark public interest.³¹⁵ The Governments of Oman, Kuwait, Bahrain, the United Arab Emirates, and Qatar all allow unrestricted access to the Internet.³¹⁶

III. THE EUROPEAN UNION SHOULD ADOPT THE
COMMISSION RECOMMENDED PICS BASED RATING
SYSTEM AND THIS SYSTEM SHOULD
PROVIDE THE BASIS FOR AN
INTERNATIONAL AGREEMENT

The European Union should adopt the Commission recommended PICS-based rating system³¹⁷ because it is both technically the best way to prevent users from accessing undesirable content and is consistent with EU goals of freedom of speech and the four freedoms.³¹⁸ Countries around the world could use this rating system to prevent their citizens from accessing undesirable content.³¹⁹ PICS already has international support³²⁰ and, therefore, the international community should use the rating system as the basis for an international agreement on Internet regulation.

312. See Gauch, *supra* note 201, at 1 (noting views of Internet by such Middle Eastern governments as Jordan, Egypt, and Saudi Arabia).

313. Wendy Grossman, *Connected: A Grip on the Net Analysis Britain's New Internet Control Scheme is Based on a Self-Regulatory Approach*, DAILY TELEGRAPH, Oct. 1, 1996, at 12.

314. Stuart Wavell, *Closed Societies Opened by Internet Genie*, THE TIMES (LONDON), Sept. 3, 1995, at 4.

315. See Gauch, *supra* note 201, at 1 (characterizing Egypt as receptive to Internet).

316. *US Firm Sprint to Provide Internet Service to Oman*, AGENCE FR.-PRESSE, July 24, 1996, at 1.

317. See *supra* notes 126-51 and accompanying text (defining PICS and setting forth technical description of PICS).

318. See *supra* notes 175-95 and accompanying text (discussing EU law).

319. See *supra* notes 16, 102-07 and accompanying text (noting undesirable content).

320. See Commission Communication, *supra* note 13, COM (96) 487, at 21-23 (noting international support for PICS).

A. *The EU Should adopt the Commission's Recommendation For a PICS based Rating System*

The European Union should adopt the Commission's recommendation for a PICS based rating system because it is both the best way technically to shield users from objectionable content³²¹ and furthers the goals of EU law including freedom of speech and the four freedoms.³²² There are other technical ways to shield users.³²³ None, however, is as consistent with the goals of EU law as the PICS based rating system.

1. *The Most Effective Way to Shield Users from Undesirable Content is to Prevent the Retrieval of Content with a Rating System Based on PICS*

Preventing the retrieval of undesirable content³²⁴ is the most effective way to shield users from undesirable Internet content. Preventing the transmission of undesirable content to the Internet³²⁵ or removing undesirable content from the Internet are also options,³²⁶ but they are not as effective as preventing retrieval. There are several ways to prevent retrieval,³²⁷ but a rating system based on the PICS technology is the best way for governments to prevent the retrieval of undesirable content in a consistent and informed manner.

a. *Preventing the Transmission of Undesirable Content to the Internet is not an Effective Way to Shield Users from Undesirable Content*

Censors can prevent the transmitting of undesirable content to the Internet by stalling content in transit and then scanning the content to determine if it is undesirable.³²⁸ To determine the content's desirability, censors would have to scan the

321. *See supra* notes 111-74 and accompanying text (relating methods of shielding users from undesirable content).

322. *See supra* notes 175-95 and accompanying text (detailing EU law).

323. *See supra* notes 111-51 (discussing methods of discerning whether Internet addresses contain undesirable content and whether Internet content is undesirable).

324. *See supra* notes 162-74 (detailing preventing retrieval).

325. *See supra* notes 156-58 (relating preventing transmission of content to Internet).

326. *See supra* notes 159-74 (discussing removal of content from Internet).

327. *See supra* notes 162-74 (noting methods of preventing retrieval).

328. *See supra* notes 156-58 (relating stalling and scanning of content before it reaches Internet).

content for key words or phrases and view each piece of content for undesirable audio or visual displays.³²⁹ Because of the significant delays caused by this approach, no country can use this without impeding the flow of information to the Internet.³³⁰

b. Removing Undesirable Content from the Internet Is Not an Effective Way to Shield Users From Undesirable Content

Removing content from the Internet as a method of protecting users from undesirable content works well with illegal content. When the French Government forced an ISP to remove a web page containing undesirable content, the Government simply enforced the law.³³¹ If content on the Internet violates copyright law, for example, removal of the content may further judicial goals. That the illegal content happens to be on the Internet does not affect the legality of the content.³³² The problem remains, however, that users may place content on servers in countries outside of the influence of a particular government seeking the ban.³³³

When content is legal but may be inappropriate for some group of citizens to access, removal of the content may not be the best alternative. If content is inappropriate for children to access,³³⁴ for example, but legal for adults to access, removal of the content from the Internet would prevent adults from accessing legal content.³³⁵ A limitation on access to legal content would chill the free flow of ideas on the Internet.

Another problem with the removal of content by a country's government is that content providers can place the same content on the Internet from a place where that government does not

329. *Id.*

330. See *supra* note 158 (detailing delays caused by stall and scan approach).

331. See *supra* notes 218-21 (discussing France's actions).

332. See Commission Communication, *supra* note 13, COM (96) 487, at 10 (noting that users remain subject to laws of Member States while conducting activities on Internet).

333. See *supra* notes 218-21 (detailing French Government's removal of undesirable content from French servers, and content reappearance on servers outside France).

334. See *Shea ex rel. American Reporter*, 930 F. Supp. at 932 (noting that, for example, sexually explicit content may be undesirable for children to access).

335. *American Civil Liberties Union*, 929 F. Supp. at 849 (noting that the CDA, while protecting children from undesirable content, may prevent adults from accessing legal content).

have jurisdiction.³³⁶ Countries have no direct control over content that users place on the Internet through ISPs in other countries.³³⁷ Thus, even if a particular country removed all undesirable content originating within its boundaries, users could still access the same or similar content that other countries' users have sent to the Internet.³³⁸ This occurred when France blocked a web page containing a banned book and users subsequently placed the book on web pages originating in other countries.³³⁹ Even with a worldwide agreement regarding content-retrieval, this problem would probably still exist because concluding an agreement to remove content that any country found illegal is highly improbable in that many governments might construe such an agreement as infringing on national sovereignty.

c. Preventing Retrieval of Undesirable Content is the Most Effective Way to Shield Users from Undesirable Content

There are several ways to prevent the retrieval of content from the Internet, including blacklisting,³⁴⁰ whitelisting,³⁴¹ word and character search,³⁴² prompting,³⁴³ and rating.³⁴⁴ They all work to varying degrees.³⁴⁵ Only a rating based on PICS, however, will effectively prevent retrieval.

i. Blacklisting is an Inadequate Method to Prevent Retrieval
Many countries have tried blacklisting with varying results.

336. See Uhlig, *supra* note 138, at 8 (noting that users can access ISPs located abroad).

337. See *id.* at 8 (noting that governments have no control over ISPs located abroad).

338. *Id.* at 8.

339. See *supra* notes 219-22 and accompanying text (relating France's blocking of web page containing banned book).

340. See Commission Communication, *supra* note 13, COM (96) 487, at 20 (defining blacklisting as act of blocking users access to Internet addresses known to contain undesirable content).

341. See *id.* at 20 (defining whitelisting as allowing access only to sites known not to have undesirable content).

342. See *supra* notes 118-21 and accompanying text (detailing use of word and character search).

343. See *supra* note 114 and accompanying text (discussing prompting).

344. See *supra* notes 111-51 (detailing methods of discerning whether Internet addresses contain undesirable content).

345. See *supra* notes 111-51 (relating degree of effectiveness of various methods of discerning whether Internet addresses contain undesirable content).

A significant problem with blacklisting is that censors can only block a particular site's address but not the content itself.³⁴⁶ If users put the same or similar content on another, non-banned, Internet address, users may still access the content.³⁴⁷ If ISPs blacklist certain newsgroups' addresses, for example, as German ISPs did,³⁴⁸ users would be able to circumvent the blacklist by accessing the newsgroups at a non-banned Internet addresses containing copies of the newsgroups, or users could access an automated server that transmits newsgroup articles on request via e-mail.³⁴⁹ Accordingly, blacklisting is not an effective way of shielding users from undesirable content.

England, Singapore, and Vietnam have tried blacklisting by threatening to prosecute or close down ISPs that allow users to access Internet sites containing undesirable content.³⁵⁰ China has tried to accomplish blacklisting through the use of proxy servers.³⁵¹ Singapore has also tried and is now decreasing its use of proxy servers.³⁵²

ii. Whitelisting is an Inadequate Method to Prevent Retrieval

As whitelisting allows retrieval of content only from sites known to contain desirable content,³⁵³ it does not fit the needs of most Internet users. Whitelisting works well for parents who only want their children to access sites that they have pre-approved.³⁵⁴ Countries that desire to limit citizens' access only to sites that censors had pre-approved could also use whitelisting. Most users, however, need to be able to access sites when they do

346. See *supra* note 165 and accompanying text (noting that blacklisting identifies offending sites not by content, but by address).

347. See *supra* notes 138-216 and accompanying text (detailing users accessing banned content on non-banned Internet addresses).

348. See *supra* notes 138-216 and accompanying text (discussing Germany blacklisting certain newsgroups).

349. Diamond, *supra* note 216, at 70.

350. See *supra* notes 226-27 (detailing England threatening its ISPs); see *supra* note 287 and accompanying text (relating Singapore threatening its ISPs); see *supra* note 299 and accompanying text (detailing Vietnam threatening its ISPs).

351. See *supra* notes 307-08 and accompanying text (detailing China's use of proxy server).

352. See *supra* notes 285-86 and accompanying text (discussing Singapore's use of proxy server).

353. See *supra* note 162-63 and accompanying text (relating whitelisting).

354. See *supra* note 174 and accompanying text (noting that software based on whitelisting technique enables user to block all sites except for those that user specifically chooses to make available).

not know whether the site contains undesirable content. Whitelisting is thus inadequate for these users as it limits them to only sites on a pre-approved list of sites.

iii. Word and Character Search is an Inadequate Method to Prevent Retrieval

The word and character search method of determining if content is undesirable, which German police used when they required CompuServe to block access to newsgroups containing the word sex,³⁵⁵ and which parents use with certain software that protects their children,³⁵⁶ has major faults. As addresses do not necessarily contain any words or characters indicating their content,³⁵⁷ this method may not be able to effectively determine whether content is undesirable. A web page that has WWW.JK.COM as its address, for example, may contain sexually explicit content. None of the words or characters in the address, however, indicate the sexual nature of the content.

Some words or characters, moreover, often have both sexual and non-sexual meanings. Words and character searches may actually block desirable content while trying to prevent access to undesirable content.³⁵⁸ When America Online³⁵⁹ banned the use of the word "breast," breast-cancer survivors quickly protested because it blocked access to sites that the survivors wanted to access.³⁶⁰ When the White House's web page referred to the president's family as the first couple, some software prevented access to the web page because "couples" was a trigger word for that software.³⁶¹

355. See *supra* notes 212-16 and accompanying text (detailing German police requiring CompuServe to block certain newsgroups).

356. See *Shea ex rel. American Reporter*, 930 F. Supp. at 932 (noting that parents use software based on using characters or words that comprise Internet addresses to determine if addresses contain sexually explicit content to protect their children).

357. See *supra* note 112 and accompanying text (explaining that addresses do not necessarily provide information about content).

358. See *Diamond*, *supra* note 216, at 70 (positing that words could have double meanings).

359. See *Bee*, *supra* note 120, at D1 (noting that America Online provides access to both Internet and its own proprietary content for fee).

360. See *Diamond*, *supra* note 120, at 70 (detailing results of America Online's banning use of word breast).

361. See *id.* (relating problem resulting from use of word "couples" on White House web page).

iv. Prompting is an Inadequate method to Prevent Retrieval

Although Technology exists for a content provider to prompt users who access content through the WWW, this method suffers from a serious drawback.³⁶² Through prompting, content providers can inform users about the type of content that the users are attempting to access,³⁶³ and content providers can query users to decide whether to grant access to the content.³⁶⁴ Countries could mandate the use of prompting to inform users of the type of content that the users are attempting to access, enabling users to make an informed decision about whether to access the content. This would leave the decision of whether to access content up to users. Alternatively, countries could place the burden on the content providers, as the United States did,³⁶⁵ to decide whether to allow users to access content based on whether a particular user has the legal right to access particular content. Content providers could query users to determine, for example, if the users were of a legal age to access particular content.³⁶⁶

Prompting, however, has a technically significant problem that makes it an ineffective method of shielding users from undesirable content.³⁶⁷ Only the WWW technology is capable of prompting users.³⁶⁸ Content providers, therefore, cannot use prompting to warn or query users attempting to access content with any other Internet exchange technology.³⁶⁹ As such, prompting is inadequate to address the needs of regulating undesirable Internet content.

362. See *supra* note 122 and accompanying text (detailing prompting use on web pages).

363. See *supra* note 122 and accompanying text (discussing use of prompting to provide users with information).

364. See *supra* notes 123-24 and accompanying text (detailing use of prompting to screen users before allowing access to web pages).

365. See *supra* notes 248-49 and accompanying text (relating U.S. federal law that criminalizes sending or displaying patently offensive sexual or excretory activities or sexual organs to persons under age 18).

366. See *supra* notes 123-25 (detailing use of prompting to screen users before allowing access to content).

367. See *supra* note 125 and accompanying text (discussing technical limitations of prompting).

368. See *supra* note 125 and accompanying text (noting that no technology except WWW is able to prompt).

369. See *supra* notes 68-100 and accompanying text (detailing different Internet exchange technologies).

v. A Rating System Based on PICS is the Best Way to Prevent the Retrieval of Content

A PICS based rating system would provide users and censors with an effective way to prevent the retrieval of undesirable content.³⁷⁰ PICS insures uniformity in rating so that all software can understand the ratings.³⁷¹ Users could access content that has a rating acceptable to them.³⁷² Censors and parents could allow access only to content that has an acceptable rating.³⁷³

A PICS based rating system also avoids many of the pitfalls of the other technological methods. Unlike blacklisting and whitelisting, where censors can only block a particular site's address but not the content itself,³⁷⁴ PICS allows blocking of the actual content.³⁷⁵ Whereas the word and character search method is inadequate because addresses do not necessarily contain any words or characters indicating their content,³⁷⁶ any address or content could contain a PICS rating.³⁷⁷ Unlike the method of prompting users, PICS is not limited to use with WWW technology.³⁷⁸

2. Commission's Recommendation For a PICS Based Rating System is Consistent with EU Law

EU law devised to shield users from undesirable content must balance the protection of minors and others³⁷⁹ with the EU

370. See *supra* notes 116-27 and accompanying text (detailing rating).

371. See *supra* note 130 and accompanying text (noting that PICS are technical specifications that provide Internet standards for rating).

372. See *supra* notes 147-50 and accompanying text (relating process to block access to content based on content's rating).

373. See *supra* notes 147-50 and accompanying text (detailing process of blocking access to content based on content's rating).

374. See *supra* note 165 and accompanying text (noting that blacklisting identifies offending sites not by content, but by address); *supra* note 174 and accompanying text (noting that software based on whitelisting technique enables user to block all sites except for those that user specifically chooses to make available).

375. See *supra* notes 147-50 and accompanying text (discussing process of using PICS to block access to content based on content's rating).

376. See *supra* note 112 and accompanying text (explaining that addresses do not necessarily provide information about content).

377. See *supra* notes 147-50 and accompanying text (relating process of placing PICS rating on content or address).

378. See *supra* note 125 and accompanying text (noting that no technology except WWW is able to prompt).

379. See Green Paper, *supra* note 15, COM (96) 483 Final at 6 (noting that protection of minors and adults is fundamental concern when proposing media regulation).

principle of freedom of expression.³⁸⁰ Such a law, in addition, would have to accommodate the common market's four freedoms.³⁸¹ The PICS based rating system manages to further all of these goals without compromising any of them.

A PICS-based rating system appropriately protects minors and others because it enables parents, educators, and other users to determine what type of content the users or others in the users' care can access.³⁸² This insures the attainment of the EU goal of protection of minors, because parents, educators, and others can block minors' access to harmful content.³⁸³ This also provides a way for adults to insure that they themselves will not accidentally retrieve undesirable content on the Internet.³⁸⁴

A system other than one allowing users to determine the types of content they can access might interfere with the freedom of expression.³⁸⁵ If the Member States prevented users from placing undesirable content on the Internet,³⁸⁶ those Member States would be interfering with users' freedom of expression³⁸⁷ by preventing them from engaging in lawful speech. Although freedom of expression is not absolute,³⁸⁸ the Commission proposed PICS based rating system eliminates the need to limit freedom of expression on the Internet because the system allows users to express themselves through the content placed on the Internet while enabling the protection of users from undesirable content.

A system other than the Commission recommended PICS

380. See *supra* notes 22, 194-97 and accompanying text (detailing EU freedom of expression).

381. See *supra* notes 189-93 and accompanying text (discussing free movement of goods, services, persons, and capital)

382. See *supra* notes 147-51 and accompanying text (describing process of blocking access to certain content based on PICS rating).

383. See *supra* notes 147-51 and accompanying text (noting the process of blocking access to content based on PICS rating).

384. See *supra* note 147-51 and accompanying text (detailing use of PICS to prevent access to undesirable content).

385. See *supra* notes 22, 194-97 and accompanying text (relating EU freedom of expression).

386. See *supra* note 156 and accompanying text (detailing how country could prevent users from placing content on Internet).

387. See *supra* notes 191-95 and accompanying text (discussing freedom of expression).

388. See *supra* notes 195-97 and accompanying text (explaining that freedom of expression right is subject to limitations for certain reasons, protection of health or morals, protection of minors, and prevention of crime).

based rating system might also interfere with the EU common market.³⁸⁹ If, for example, a Member State either prevented the transmission of undesirable content to the Internet³⁹⁰ or removed content from the Internet,³⁹¹ the Member State might be interfering with the free movement of goods in that the goods, i.e. the content, could not flow freely throughout the European Union.³⁹² That Member State might also be interfering with the free movement of capital if a fee is required to receive the goods.³⁹³ Moreover, if a Member State were to prevent content providers from selling services, sexual or otherwise, on the Internet, that Member State might be impeding the free flow of services.³⁹⁴

A system where a Member State could choose what type of content users could receive from the Internet would also be inconsistent with EU law. Doing so would impede the free flow of ideas, thus impinging on the right to freedom of expression.³⁹⁵ Doing so would also interfere with the flow of services, goods, and capital by preventing the flow of certain types of content.

EU Member States could place the burden on the content providers, as the United States did,³⁹⁶ to decide whether to allow users to access content based on whether a particular user has the legal right to access particular content. If Member States did so, however, the content provider's only real option for escaping liability would be using the inadequate technology of prompting.³⁹⁷ Prompting, which would attain the goal of protecting minors and others, is inadequate because it only works with the

389. See *supra* note 188 and accompanying text (discussing EU common market).

390. See *supra* note 156 and accompanying text (detailing how country could prevent users from placing content on Internet).

391. See *supra* notes 152-74 and accompanying text (discussing how country could remove content from Internet).

392. See *supra* note 190 and accompanying text (detailing free movement of goods).

393. See *supra* note 190 and accompanying text (relating free movement of capital as one of four freedoms of European Community).

394. See *supra* note 191 and accompanying text (detailing free movement of services in context of European Community).

395. See *supra* notes 195-97 and accompanying text (discussing freedom of expression in European Union as encouraging free flow of ideas).

396. See *supra* notes 248-49 and accompanying text (detailing U.S. federal law that criminalizes sending or displaying patently offensive sexual or excretory activities or sexual organs to persons under 18).

397. See *supra* notes 122-25 and accompanying text (describing prompting on web pages).

WWW and none of the other Internet exchange technologies.³⁹⁸ Content providers could prompt users, informing users about the type of content that they are attempting to access,³⁹⁹ or query users to decide whether to grant them access to the content.⁴⁰⁰

Even if prompting could work with all Internet technologies, requiring content providers to determine if users have the legal right to access specific content contravenes the freedom of expression and would impede the flow of commerce on the Internet. Such a requirement could only work if users provided some type of proof that they have the legal right to access certain types of content.⁴⁰¹ The U.S. Congress proposed the use of an adult identification code or credit card as proof that a person is of legal age to access certain types of content.⁴⁰² An adult identification code would increase the transaction cost of users accessing web pages due to the cost of designing and maintaining identification code verification services or using third party services.⁴⁰³

Forcing content providers to absorb the cost of verifying every user's legal right to access certain types of content might deter them from transmitting content to the Internet, in effect chilling speech.⁴⁰⁴ Passing along the cost to users might deter users from accessing those web pages, again chilling speech.⁴⁰⁵ A decrease in users accessing web pages also would hurt commercial content providers because they depend on a demonstration that their web pages are widely available and frequently vis-

398. See *supra* note 125 and accompanying text (noting prompting only works with WWW).

399. See *supra* note 122 and accompanying text (relating use of prompting to provide users with information).

400. See *supra* notes 122-25 and accompanying text (detailing use of prompting to screen users before allowing access to web pages).

401. See *supra* notes 122-25 and accompanying text (discussing use of prompting to screen users by predicating access on showing of identification).

402. See *supra* note 255 and accompanying text (detailing U.S. Congress, in CDA, providing defense to person that has restricted access to CDA prohibited communication by requiring use of some type of identification, including credit card, debit account, adult access code, or adult personal identification).

403. See *supra* note 123 and accompanying text (relating cost of designing and maintaining identification code verification services or using third party services).

404. See *American Civil Liberties Union*, 929 F. Supp. at 867 (finding CDA to stifle speech on Internet).

405. *Id.*

ited for advertising revenue.⁴⁰⁶ A credit card requirement also would increase the transaction cost of users accessing web pages due to the cost of credit card validation,⁴⁰⁷ again impeding freedom of expression and the flow of commerce. Predicating access on possession of a credit card number, moreover, would completely bar users who are unable to obtain credit cards from accessing content.⁴⁰⁸ Thus, even if a user had the legal right to access content, that user would not be able to access content merely because he or she does not possess a credit card.

C. *International Rating System Based on PICS*

Global implementation of the PICS based rating system would provide uniformity in rating⁴⁰⁹ and thus represents a first step in instituting an effective system to shield users from undesirable content. Several additional steps are needed in order to create an effective worldwide system of shielding users from undesirable content, including creating uniform categories for rating Internet content,⁴¹⁰ mandating that all users placing content on the Internet rate that content and notify third party rating services of all new content posted on the Internet,⁴¹¹ and actively encouraging third party rating services.⁴¹² Although the worldwide system has some potential problems, on the whole, it would be an effective system.

1. Rating System

Global implementation of the PICS based rating system is essential for an effective rating system because it would create worldwide uniformity in regulating the Internet as opposed to merely uniformity within the European Union. If only EU Member States implemented the PICS rating system, for instance, parents would still not know if content that users posted in other

406. *See id.* at 821 (detailing advertising revenue of web pages).

407. *See supra* note 123 and accompanying text (discussing credit card validation and noting that validation costs from sixty cents to over one dollar per transaction).

408. *See supra* note 124 and accompanying text (detailing credit card validation costs).

409. *See supra* note 130 and accompanying text (noting that PICS are technical specifications that provide Internet standards for rating).

410. *See PICS Rating Services, supra* note 140 (providing WWW address containing links to several rating services that provide different ways to categorize content).

411. *See supra* note 145 and accompanying text (relating rating services).

412. *See supra* note 145 and accompanying text (detailing use of rating services).

countries was suitable for their children.⁴¹³ The Commission, realizing the problem with anything less than a worldwide plan, advocated discussions with multinational organizations on regulating the Internet.⁴¹⁴ While implementation of the PICS technology is an important first step, an effective worldwide system of shielding users from undesirable content calls for several additional steps.

Countries must mandate that all groups rating content on the Internet use only the PICS technology to create uniformity in rating. If raters used technology other than PICS, a particular user's software might not be compatible with that technology, making it impossible for the software to discern the rating on some content.⁴¹⁵ With a worldwide rating system based on PICS, users and censors could use PICS compatible software, ensuring that the software could discern content ratings.

Countries must establish categories for rating Internet content in order to create uniformity in categorizing content.⁴¹⁶ Like the selection of a rating technology, uniformity ensures that software can readily identify undesirable content. Countries must establish enough categories to satisfy the needs of the censors without creating so many categories that rating content is overly burdensome.

An effective PICS-based system also would require countries to mandate that content providers notify third party rating services of all new content posted on the Internet.⁴¹⁷ This mandatory regulation will enable third party raters to rate the content quickly. To streamline the notification process, content providers could notify just one site and that site would automatically notify all third party rating services.

In order for users to find a rating service with which they feel comfortable, countries must actively encourage third party

413. See *supra* note 299 (discussing that inserting ratings such as tags is unfeasible because implementation would need worldwide consensus to be effective and there is currently no worldwide consensus on any such label).

414. See *supra* note 242 and accompanying text (detailing EU's proposals).

415. See *supra* note 147 and accompanying text (relating compatibility of software with PICS).

416. See *PICS Rating Services*, *supra* note 140 (providing WWW address containing listing of links to several rating services providing different ways to categorize content).

417. See *supra* notes 140-47 and accompanying text (detailing use of third party rating services).

rating services.⁴¹⁸ As categorization of content is a subjective process, countries must encourage diverse groups with different political, social, and religious views to operate rating services in order to provide more options to users. Individual countries could act as third party rating services. A worldwide body could finance rating services or rating services could charge a nominal fee to their users. Rating services should not charge content providers for the rating of content because the fee may discourage users from putting content on the Internet, inhibiting the free flow of speech.

A worldwide system of PICS-based rating would enable effective shielding of undesirable content. Once they set up this system, participating governments could remain uninvolved in the regulation of legal but undesirable content on the Internet insuring freedom of expression in these places. Parents, educators, and others could choose whether to shield themselves, their families, or their students from accessing undesirable content by specifying categories of rating services of their own choice, allowing individual users to decide what is best for themselves and those in their care.⁴¹⁹

If the European Union and governments choose, they can take additional action to remove illegal content from the Internet.⁴²⁰ Governments, such as those in China⁴²¹ and Singapore,⁴²² that desire stronger control over what their citizens access, can prevent their citizens from accessing certain types of content by using their own rating service with a proxy server⁴²³ that does not allow users to access specified content based on the global standard of PICS-based rating.⁴²⁴ Countries could do this by mandating that ISPs only allow users to contact sites that

418. See *supra* note 239 and accompanying text (discussing Commission's recommendations calling for European Union to establish multiple rating services).

419. See *supra* note 145 and accompanying text (detailing that parents can use rating services that they trust).

420. See *supra* notes 223-36 (relating Commission's recommendations for combating illegal Internet content).

421. See *supra* notes 303-08 and accompanying text (detailing China's actions in regulating Internet content).

422. See *supra* notes 300-02 and accompanying text (discussing Singapore's regulations concerning Internet).

423. See *supra* note 170 and accompanying text (noting that proxy servers are computers that screen all requests made by users and block access to banned sites).

424. See *supra* notes 147-50 and accompanying text (detailing blacklisting, process of preventing access to Internet addresses).

do not have undesirable content.⁴²⁵ ISPs, in turn, could do this by using PICS compatible software and a particular rating service.⁴²⁶ Countries, alternatively, could suggest or mandate that users use software preset not to accept content of a certain type and work only with government approved rating services.⁴²⁷

2. Potential Problems with Rating System

Implementation of the worldwide rating system has three potential problems. Firstly, PICS will not work with e-mail.⁴²⁸ To determine if e-mail contains undesirable content, a government or other agency could stall e-mail messages in transit and then scan them for key words or phrases.⁴²⁹ Such a process, however, would cause significant delays in the forwarding of e-mail.⁴³⁰ Moreover, if users encrypt the content, the stall and scan approach will not work as stalling and scanning cannot discern encrypted content.⁴³¹ Regulating e-mail, however, would be the most intrusive form of government regulation on the Internet as e-mail, being analogous to a letter, is a private correspondence between two or more users. Regulating such correspondences would inhibit the free flow of ideas, as users would be afraid to communicate in what should remain a private arena.

Secondly, countries that want to censor their users, even if these countries mandate that ISPs use certain rating services, would still have the problem of users accessing ISPs that are located in other countries.⁴³² Perhaps part of the worldwide system would include mandating that ISPs could only allow access to users from the country where the ISPs were situated. That is,

425. See *supra* notes 147-50 and accompanying text (relating use of PICS compatible software to prevent access to Internet addresses).

426. See *supra* note 147-50 and accompanying text (detailing PICS compatible software ability to prevent access to Internet addresses).

427. See *supra* notes 140-46 and accompanying text (asserting that countries can act as their own rating service or use rating service they trust).

428. See *supra* note 138 and accompanying text (discussing PICS not working with e-mail).

429. See *supra* note 157 and accompanying text (detailing stall content in transit).

430. See *supra* note 158 and accompanying text (relating delay caused by stalling content in transit).

431. See *supra* note 158 and accompanying text (stating that stall and scan approach cannot work with encrypted e-mail).

432. See Uhlig, *supra* note 138, at 8 (noting that governments have no control over ISPs located abroad).

if an ISP found that a user's telephone number was from another country, the ISP would deny the user access.

Finally, as new content is continuously being put on the Internet,⁴³³ there will inevitably be a lag time between the placing of the content on the Internet and a third party rating the content.⁴³⁴ Users, however, could trust that the self-raters rated the content adequately, keeping in mind that fear of a fine deters content providers from rating inadequately. Users, moreover, could program their software not to access any content that a third party rating service has not yet rated.⁴³⁵

CONCLUSION

The PICS based rating system, being both technically feasible and consistent with EU law, provides the best way to shield users from undesirable Internet content. The proposed global PICS based rating system will allow each country to use the system in a way that will conform with its laws. Without the use of this system, use of the Internet will continue to expose minors and others to undesirable content.

433. See *Shea ex rel. American Reporter*, 930 F. Supp. at 932 (detailing constant stream of new content to Internet).

434. See *supra* notes 140-46 and accompanying text (discussing process of rating content).

435. See *supra* notes 147-50 and accompanying text (detailing process of preventing access to Internet addresses using PICS compatible software).