Redesigning the Internet for Content Regulation

Lawrence J. Appleman

DISSERTATION.COM

Boca Raton

Redesigning the Internet for Content Regulation

Dissertation.com
Boca Raton, Florida
USA • 2008

ISBN-10: 1-59942-694-3
ISBN-13: 978-1-59942-694-5

Table of Contents

1) Introduction

As a successful collaboration of scientists, engineers, and policymakers from academia, government, and commerce, the Internet does exactly what it was designed to do – allow unhindered transmission of content from any location to any other location, even if portions of the network are disconnected. As the Internet has grown and expanded throughout the world, its underlying technologies have evolved to solve additional problems and to provide new and unexpected applications. As these technologies continue to evolve, an important issue receives far too little technological attention: revising Internet standards to allow for limitation and control of transmission of content. This dissertation proposes that policymakers set control of content as a high-priority goal for research into future Internet standards.

As a foundation for this proposal, part 2 of this dissertation outlines the history of the Internet's technological development, including major milestones in its development and several examples of recent and ongoing efforts to evolve the Internet's next generation; describes the interaction of legal issues with scientific and engineering efforts; and identifies the underlying legal foundation for content regulation and restriction. In part 3, detailed examples are provided to show the scope, breadth, and reach of legal efforts to regulate and restrict Internet content. To demonstrate the consequences of the current Internet's lack of support for content regulation, part 4 reports on present ways in which governments and commercial interests restrict transmission of Internet content, by technologies which circumvent Internet standards, by practical means such as preventing access physically or monitoring use manually, or by strong enforcement of strict laws and regulations. Part 5 describes how current efforts to control Internet content are undermined by techniques that further subvert Internet standards. A summary of jurisprudential theory and legal philosophies regarding Internet content is provided in Part 6, to explain some of the reasons that content regulation has not been a priority during the development of the Internet. How future Internet priorities are set, how research is administered, and how Internet standards are changed, are described in part 7. Finally, part 8 identifies some current priorities for Internet research, proposes that content regulation should be given far more attention, and suggests ways in which such efforts may proceed.

2) Background

a) History and architecture of the Internet

i) Arpanet (1969)

In its earliest incarnation, the Internet was intended to provide effective transmission of content and to prevent interruptions, changes, and diversions of that content. The Internet's birth is credited to computer researchers at the University of California, Los Angeles, who in 1969 were investigating the best ways to transfer data among computers using networks.[1] Their effort was called the Advanced Research Project Agency Network ("ARPANET"),[2] with the goal of providing communication among government and university computers using overlapping channels, so that communication would be possible even if some portions of the network were destroyed by war or natural disaster.[3] Intentional limitation of Internet content perforce conflicts sharply with that original goal.

ii) The Internet (circa 1973-1983)

As the Internet expanded its users outside of government and universities, a fundamental architecture took shape that is still in use today. The technical basis for the Internet is a structure of four layers, which are conceptualized as existing one atop the other.[4] Most users of the Internet see only the top layer – the content layer – that presents material such as websites. Below the content layer is the application layer, which consists of software that makes content available, such as browser programs for viewing websites and media player programs for video and audio content.[5] Such application software may be open-source, with code available and readable by the public, or may be proprietary, with code kept private and protected as a trade secret.[6] The logical layer is next, comprised of the communication standards, such as the Transport, Control Protocol and the Internet Protocol (TCP/IP), which allow disparate computers to send and receive data.[7] This logical layer is a collection of "protocols": global protocols such

---

[1] Jesdanun, Anick, Thirty-five years old, Internet remains a work in progress, Associated Press, August 27, 2004, LEXIS NEWS library, AP file

[2] O'Rourke, Maureen, Fencing cyberspace: drawing borders in a virtual world, 82 Minn. L. Rev. 609, 616 (1998).

[3] Reno v. ACLU, 521 U.S. 844, 849-50 (1997).

[4] Weiser, Philip J., The Internet, innovation, and intellectual property policy, 103 Colum. L. Rev. 534, 541 (2003).

[5] *Id.* at 542 (2003).

[6] Lane, Thomas A., Of hammers and saws: the toolbox of federalism and sources of law for the web, 33 N.M.L. Rev. 115, 119 (2003).

[7] Speta, James B., A common carrier approach to Internet interconnection, 54 Fed. Comm. L.J. 225, 243-47 (2002).

as the Internet Protocol, which every computer must support in order to use the Internet; public protocols which are openly available and are needed only for specific activities, such as the Internet Relay Chat Protocol for instant messaging; and private protocols which are privately owned and unpublished, such as file formats for proprietary computer programs.[8] At the bottom of this conceptual structure is the physical layer: wires, fiber optic cables, and other modes of transmission from one place to another.

The principal computer programs and communication standards for the Internet were developed through the collaborative efforts of academics and engineers, with substantial support from the United States government.[9] As the Internet grew, commercial enterprises began to participate as well, with continuing support from the government. As an illustration, when the ARPANET protocols were officially retired in 1983, the National Science Foundation began providing support for commercial Internet research in the mid-1980s and continued to provide increasing support until the mid-1990s.[10]

A significant milestone in the evolution of the Internet is the ongoing deployment of Internet Protocol version 6 (IPv6), to replace the current widespread de facto standard Internet Protocol version 4 (IPv4).[11] The main motivation for development of IPv6 was that the number of computer addresses available in IPv4 is limited to approximately 4.3 billion unique addresses, less than the Earth's human population.[12] IPv6 allows four times as many digits for each address, which permits approximately "670 quadrillion (thousand trillion) unique addresses for every square millimeter of the Earth's surface";[13] further, IPv6 adds technical improvements to the Internet for better routing and configuration of networks.[14] As with other new generations of the Internet, IPv6's improvements do not focus on solutions for control and regulation of Internet content.

---

[8] Lane, Thomas A., *supra* note 6 at 118.

[9] Weiser, Philip J., *supra* note 4 at 546.

[10] Froomkin, A. Michael, Wrong turn in cyberspace: using ICANN to route around the APA and the constitution, 50 Duke L.J. 17, 55 (2000).

[11] Helms, Shawn C., Translating privacy values with technology, 7. B.U. J. Sci. & Tech. L. 288, 299 (2001).

[12] Roush, Wade, The Internet reborn, Technology Review, vol. 106, no. 8, p. 32, Oct. 1, 2003.

[13] *Id.*

[14] IPv6, http://www.ipv6.org (visited 9/15/04).

iii) Mbone (1992)

In order to solve the problems of handling transmission of extremely large quantities of data to multiple simultaneous recipients, the Multicast Backbone (also known as Mbone)[15] was developed by the Internet Engineering Task Force,[16] because Internet standards are not best for this use, as they focus on sending each specific packet of data to a single destination.[17] Mbone is another example of Internet solutions that provide more effective transmission of content with little attention paid to limiting content.

iv) Internet2 (1996)

Because the physical infrastructure of the Internet did not allow sufficient bandwidth for envisioned collaborative efforts, an academic consortium named Internet2 was formed "to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet."[18] Internet2's membership is limited to colleges and universities in the United States only,[19] and while it continues today as an active platform for academic research, industry analysts do not see it as an influential model for use by the general public.[20]Internet2's network, called Abilene,[21] allows transmission of content many times faster than the conventional Internet, and serves as an environment for continued academic research into new technologies and new forms of Internet content, such as three-dimensional virtual environments, and means of transmitting the senses of touch and smell[22] – looking at ways of transmitting additional content, not limiting or controlling Internet content.

v) Grids (1996)

In the mid-1990s, several research efforts got under way to explore linking disparate high-performance computing facilities using fast and copious network connections to form

---

[15] Eriksson, Hans, Mbone: the multicast backbone, Communications of the ACM, vol. 37, no. 8, p. 54, August 1994.

[16] *See infra* text at 7)b)ii)

[17] Roush, Wade, *supra* note 12 at p. 36.

[18] Internet2, About Internet2, http://www.Internet2.edu/about/ (visited 9/14/04).

[19] Internet2, University membership application requirements, http://members.Internet2.edu/university/RegularRequirements.html (visited 9/15/04).

[20] Lyman, Jay, Whatever happened to Internet2?, NewsFactor, Feb. 21, 2002, http://www.newsfactor.com/story.xhtml?story_id=16409 (visited 9/15/04).

[21] Abilene Backbone Network, http://abilene.Internet2.edu/ (visited 9/14/04).

[22] Holstein, William, Building the next Internet, U.S. News, Sept. 13, 1999, http://www.Internet2.edu/resources/19990913-USNews.pdf (visited 9/15/04).

"grids" that can work collectively to form virtual, massive supercomputers.[23] One such project is spearheaded by the U.S. Department of Energy and the University of Southern California;[24] another project, called TeraGrid, is funded by the U.S. National Science Foundation combines grid computer architecture with a dedicated high-speed network backbone.[25] These research-oriented environments today focus on intense analysis of the vast quantities of data that may be gathered by modern instrumentation, such as data about the human genome, drug interactions, weather patterns, and high-resolution models of the physical world;[26] like most other Internet research today, grid computing examines ways of providing additional information rather than techniques for limiting its transmission.

vi) Abone (2000)

An approach to adding flexibility and new features to the Internet, "active networking" allows information to be transmitted with instructions that control the behavior of the network, unlike today's Internet, where the network's behavior is guided by standards rather than anything contained in transmitted content.[27] To test this approach, a dedicated network has been built, funded by the U.S. Defense Department's Advanced Research Projects Agency, called the Active Network Backbone ("Abone").[28] If Internet content were to include instructions for how the network should behave, new risks and vulnerabilities to deliberate attacks would likely appear, so Abone provides not only for research into active networking's new developments, but also into managing its vulnerabilities.[29] As active networking focuses on control of the network, this technology has some potential for future research into regulation and restriction of Internet content, if policymakers set that as a priority.

vii) PlanetLab (2002)

The most recent major research effort aimed at overcoming limitations inherent in the Internet is PlanetLab, which is principally built around the concept of "smart nodes" – replacing the Internet's inflexible routers with computers capable of running programs controlled by

---

[23] TeraGrid, Frequently asked questions, http://www.teragrid.org/about/faq.html (visited 9/15/04).

[24] Roush, Wade, *supra* note 12 at p. 36.

[25] TeraGrid, *supra* note 23.

[26] *Id.*

[27] Han, Young J., Yang, Jin S., Chang, Beom H., and Chung, Tai M., SVAM: The scalable vulnerability analysis model based on active networks, Information Networking: Networking Technologies for Broadband and Mobile Networks International Conference ICOIN 2004, pp. 857-866 (2004).

[28] Roush, Wade, *supra* note 12 at p. 36.

[29] Han, Young J., Yang, Jin S., Chang, Beom H., and Chung, Tai M., *supra* note 27.

users.[30] The current emphasis is on research to allow better handling of critical – and non-critical – information, for example making it possible for all users' files and settings to be stored with archival quality on the network;[31] to enhance the Internet's security from attach, by solving problems of detection and removal of viruses and other destructive computer programs;[32] and to avoid Internet congestion and increase the Internet's speed and reliability.[33] Content regulation is not identified as a key research goal in PlanetLab's publicly available documentation,[34] but this large-scale initiative could serve as a platform for such efforts if directed by stakeholders.

b) Re-casting the protocols

i) How the Internet has evolved

The development and evolution of the Internet in its present form can be traced to the direction set by its creators and by government leadership.[35] As the Internet continues to change and grow, much of the vision that guide its growth tends to come from groups that set technical standards, such as the Internet Engineering Task Force (IETF).[36] Such technical groups, while populated by engineers and driven toward solving technological problems, must also respond to the direction of non-technical forces such as commercial interests and government policymakers.[37]

ii) Little attention to legal issues

The development of the Internet was an engineering construct designed as solving technological issues,[38] particularly to solve the problem of maintaining network connections when part of the network is unavailable. Because the Internet's current architecture does not

---

[30] Roush, Wade, *supra* note 12 at p. 30.

[31] *Id.* at p. 29.

[32] *Id.*

[33] *Id.* at p. 30.

[34] *See, e.g.*, PlanetLab, http://www.planet-lab.org/ (visited 9/15/04).

[35] Rubin, Edward L., Computer languages as networks and power structures: governing the development of XML, 53 S.M.U. L. Rev. 1447, 1449-52 (2000).

[36] Froomkin, A. Michael, Habermas@discourse.net: toward a critical theory of cyberspace, 116 Harv. L. Rev. 749, 796-817 (2003).

[37] David, Paul A. & Shurmer, Mark, Formal standards-setting for global telecommunications and information services, 20 Telecomm. Pol'y 789, 795 (1996)

[38] Hughes, Justin, The Internet and the Persistence of Law, 44 B.C.L. Rev. 359, 365 (2003).

require information to go through any specific, particular path or location, enforcing regulation or control of Internet content is particularly challenging.[39]

The theory has been proposed that the Internet's great growth, innovation, and success has been based on its openness, lack of regulation, and better-than-First-Amendment level of freedom for all content.[40] While no doubt this is a component of how the Internet works today, a strong argument can be made that other innovative and successful technologies have thrived under strict regulation. For an example that has grown contemporaneously with the Internet, we can look to mobile phone networks, which achieved analogous innovative success within a complex regulatory framework.[41]

c) Legal bases for content regulation

i) <u>preventing dissemination of harmful materials</u>

Governments maintain order by forbidden certain types of activity that cause harm to persons and property, to the stability of the government, and to the value of moral principles.[42]

The definition of what is "harmful" and the level of control – particularly control of speech and expression – varies widely among different governments. As one end of the spectrum is the United States, which has a stated policy of supporting "the broadest possible free flow of information across international borders"[43] and has applied this policy as allowing regulation of the Internet by the Internet community, with minimal government involvement.[44] Indeed, leadership in the U.S. Congress have proposed a Global Internet Freedom Act[45] that would establish a U.S. government agency to fight all state-sponsored censorship of Internet content,[46] by denouncing such censorship,[47] introducing a United Nations resolution to condemn these

---

[39] Henn, Julie L., Targeting transnational Internet content regulation, 21 B.U. Int'l L.J. 157, 159-60 (2003).

[40] *See* Lessig, Lawrence, CODE AND OTHER LAWS OF CYBERSPACE 6-8 (1999), describing a vision of the Internet as an "information commons".

[41] Weiser, Philip J., *supra* note 4 at 546.

[42] Brenner, Susan W., Complicit publication: when should the dissemination of ideas and data be criminalized?, 13 Alb. L.J. Sci. & Tech. 273 (2003).

[43] The White House, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 25 (1997).

[44] Eko, Lyombe, Many spiders, one worldwide web: towards a typology of Internet regulation, 6 Comm. L. & Pol'y 445, 452 (2001).

[45] Global Internet Freedom Act, H.R. 48, 108th Cong. (1st Sess. 2003). A nearly identical bill was introduced in the Senate, S. 3093, 107th Cong. (2d Sess. 2002).

[46] *Id.* at § 3(2).

[47] *Id.* at § 5(1).

practices,[48] and deploying technological solutions to circumvent restrictions on Internet content.[49] Commentators have suggested weaknesses of the proposed Global Internet Freedom Act: that it expressly excludes "interfer[ence] with foreign national censorship in furtherance of legitimate law enforcement aims that is consistent with the Universal Declaration of Human Rights",[50] fundamental uncertainties regarding Internet regulation, commercial opposition, and lack of appetite for the United States to take on the role of international law enforcer.[51]

In contrast, China appears to be among those nations that impose the strongest, most sophisticated and extensive controls over the flow of information, whether in print, through broadcast media, or via the Internet.[52] China's policies are specifically identified in the United States' proposed Global Internet Freedom Act as a potential target for technologies to "counter Internet jamming."[53]

---

[48] *Id.* at § 5(2).

[49] *Id.* at §§ 3-5. The proposed Global Internet Freedom Act specifically directs approaches to circumventing government-run content restrictions:

> "SEC. 3. PURPOSES
>
> "The purposes of this Act are–
>
> "(2) to establish an office …. with the sole mission of countering Internet jamming and blocking by repressive regimes;
>
> "(3) to expedite the development and deployment of technology to protect Internet freedom around the world;
>
> "(4) to authorize the commitment of a substantial portion of United States …. resources to the continued development and implementation of technologies to counter the jamming of the Internet;
>
> "(5) to utilize the expertise of the private sector in the development and implementation of such technologies, so that the many current technologies used commercially for securing business transactions and providing virtual meeting space can be used to promote democracy and freedom …
>
> "SEC. 4. DEVELOPMENT AND DEPLOYMENT OF TECHNOLOGIES TO DEFEAT INTERNET JAMMING AND CENSORSHIP.
>
> "(a) … develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming, and persecution of those who use the Internet….
>
> "SEC. 5. SENSE OF CONGRESS
>
> "It is the sense of the Congress that the United States should–…
>
> "(3) deploy, at the earliest practicable date, technologies aimed at defeating state-directed Internet censorship and the persecution of those who use the Internet."

Id.

[50] *Id.* at § 4(e).

[51] Chen, Elaine M., Global Internet freedom: can censorship and freedom coexist?, 13 J. Art & Ent. Law 229, 266 (2003)

[52] Keller, Perry, Privilege and punishment: press governance in China, 21 Cardozo Arts & Ent. L.J. 87, 87 (2003).

[53] Global Internet Freedom Act, *supra* note 45 at § 2(9).

ii) protecting individuals from harm

The existing body of law applies on the Internet, as everywhere else, to content that causes harm to others. Courts have shown themselves able to apply traditional legal theories to Internet content.

For example, the court in United States v. Hoke[54] examined a case of criminal fraud perpetrated via the Internet.[55]

Another example is provided by Japan's courts, which analyzed defamation law in the context of Internet content in the "Nifty case",[56] where messages posted in an Internet discussion forum were alleged to be defamatory.[57] The Tokyo District Court held liable for defamation the original poster of the messages, the moderator of the discussion forum, and the service provider.[58] On appeal, the Tokyo High Court[59] reversed liability for the moderator and the service provider, finding that the defamatory Internet content had been removed in a timely fashion, but affirmed liability for the poster.[60]

United States law applied to Internet content strikes a balance heavily weighted toward freedom of expression, with exceptions carved out for content that causes harm to others. One such exception is restriction of threatening content that is driven by racial animosity or includes racial slurs;[61] convictions for such content on the Internet have been upheld by United States courts.[62]

In the United States, laws protect individuals from exposure to sexually hostile environments, and the need for this protection has motivated efforts to filter content on public Internet terminals, such as at public libraries.[63]

---

[54] United States v. Hoke, CR 99-441 (C.D. Cal. Indictment filed Apr. 30, 1999)

[55] S*ee* Schwarz, Joel Michael, "A case of identity": a gaping hole in the chain of evidence of cyber-crime, 9 B.U. J. Sci. & Tech. L. 92 (2003).

[56] Nifty case, 1994-7784 Honso 24828; Hanrei Tokuhou, Tokyo-chi-han 9-5-26 [Special Report on Judgment, Tokyo District Court Judgment, May 26, 1997], 1610 Hanrei Jiho 22 (1997).

[57] *See* Yamaguchi, Itsuko, Beyond de facto freedom: digital transformation of free speech theory in Japan, 38 Stan. J Int'l L. 109, 113-14 (2002).

[58] Nifty case, *supra* note 56.

[59] Unpublished opinion (Tokyo High Ct., Sept. 5, 2001), cited in Yamaguchi, Itsuko, *supra* note 57 at 114 n. 16.

[60] Yamaguchi, Itsuko, *supra* note 57 at 114.

[61] Breckheimer II, Peter J., A haven for hate: the foreign and domestic implications of protecting Internet hate speech under the First Amendment, 75 S. Cal. L. Rev. 1493, 1507 (2002).

[62] *See* United States v. Machado, 195 F.3d 454, 457 (9th Cir. 1999).

[63] *See* Mainstream Loudoun v. Bd. of Trs., 24 F. Supp. 2d 552, 565 (E.D. Va. 1998).

iii) protecting rights of content owners

Holders of rights in intellectual property, particularly copyrights, have a strong financial interest in controlling access to Internet content.[64] These commercial interests are protected by government enforcement of intellectual property laws.[65] In the United States, for example, bills have been introduced to strengthen copyright laws applied to the Internet, and to protect the intellectual property rights of commercial interests.[66]

d) Proposal for future technological support for content regulation

The effectiveness of laws and regulations is based on whether a government has the capability of enforcing those laws and regulations.[67] The Internet today is structured so that content is moved from one place to another, and interpretation of content is the responsibility of computer programs and human beings at the ends.[68] The current architecture of the Internet does not facilitate the identification of who and where are the source and destination for content transmitted via the Internet, nor of the reasons for the content's transmission, nor of other characteristics of the content.[69] This architecture supports individuals' bypassing gatekeepers to send and receive whatever content they desire.[70]

Because current Internet architecture frustrates attempts to control content because of the particular circumstances of its creation[71], this dissertation proposes that next generations of Internet architecture deliberately include technological solutions that allow governments to enforce such control.

3) Survey of content regulation on the Internet

This section exemplifies the vast range of differences among jurisdictions when it comes to content regulation.

---

[64] "Trafficking in infringing copyrighted works … threatens lost jobs, lost income for creators, lower tax revenue, and higher prices for honest purchasers." Piracy Deterrence and Education Act, H.R. 4077 Sec. 2(2), 108th Cong. (2d Sess. 2004)

[65] *Id.* at Sec. 2(6).

[66] *E.g., id.*

[67] Goldsmith, Jack L., Against cyberanarchy, 65 U. Chi. L. Rev. 1199, 1216 (1998).

[68] Lessig, Lawrence, CODE AND OTHER LAWS OF CYBERSPACE 32 (1999).

[69] *Id.*

[70] Shapiro, Andrew L., THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 16 (1999).

[71] Zittrain, Jonathan, Internet points of control, 44 B.C. L. Rev. 653, 654 (2003).

The United States positions itself in the forefront of unfettered access to Internet content, with majority leadership in the United States House of Representatives proposing a proactive policy directed at changing other government's approaches to content regulation: [72]

> "To bring to bear the pressure of the free world on repressive governments guilty of Internet censorship, the United States should:
>
> "– Direct substantial international broadcasting resources to a global effort to defeat Internet jamming and censorship.
>
> "– Establish an Office of Global Internet Freedom within the International Broadcasting Bureau to develop and implement a strategy for defeating Internet jamming.
>
> "– Formally declare that all people have the right to communicate freely with others on the Internet.
>
> "– Formally declare that all people have the right to unrestricted access to news and information on the Internet.
>
> "– Publicly and prominently denounce state-directed practices of restricting, censoring, banning, and blocking access to information on the Internet.
>
> "– Submit a resolution at next year's U.N. Human Rights Commission annual meeting in Geneva condemning all nations practicing Internet censorship and denying freedom to access information.
>
> "– Compile and publish an annual report on countries that pursue policies of Internet censorship, blocking, and other abuses"[73]

The U.S. State Department identifies Cuba, Laos, North Korea, the People's Republic of China, Saudi Arabia, Syria, Tunisia, and Vietnam as the governments asserting the most control over their citizens' use of the Internet.[74]

China plays a key role in this discussion, because of its large number of potential and current Internet users. China, at least as recently as 2002, was second only to the U.S. in Internet

---

[72] House of Representatives Policy Statement, Establishing global Internet freedom: tear down this firewall ¶¶ 38-45, Sept. 19, 2002, http://policy.house.gov/html/news_item.cfm?ID=112 (visited 9/15/04).

[73] *Id.*

use.[75] The Chinese government shows keen interest in electronic commerce and other uses of the Internet, but appears equally – if not more – interested in ensuring that harmful Internet content is restrained.[76] "The Government continued to encourage expanded use of the Internet; however, it also took steps to increase monitoring of the Internet and continued to place restrictions on the information available. While only a very small percentage of the population accessed the Internet, use among intellectuals and opinion leaders was widespread and growing rapidly. Young persons, both urban and rural, accounted for the greatest number of Internet users. According to a quasi-government report, the number of Internet users at the end of 2002 was 59.1 million. During the year, industry officials estimated the number of users at 80-100 million, with only 27 percent of those in the urban centers of Beijing, Shanghai, and Guangzhou.[77]

Belying the notion that the Internet exists in an international space without borders, these examples demonstrate that technological, practical, and legal control can be – and is – applied by governments to ensure that the Internet is divided along conventional national boundaries.[78]

a) Forms of content regulated

i) Substantive

(1) political activism

Although very few Burmese citizens have Internet access, political content is banned for Burmese Internet users.[79] Chinese citizens have been imprisoned for political use of the Internet, such as website manager Huang Qi and students belonging to the New Youth Study Group, who are reported by the U.S. State Department to have received long prison sentences for Internet essays encouraging democracy[80] and for posting information about students who disappeared at the Tiananmen Square protests.[81] Syria's government-run Internet service provider blocks all pro-Israeli content; at least one Syrian individual has been detained for sending a political cartoon

---

[74] *Id.* at ¶ 3.

[75] Hughes, Justin, *supra* note 38 at 361 (2003).

[76] Gao, Fuping, The e-commerce legal environment in China: status quo and issues, 18 Temp. Int'l & Comp. L.J. 51, 52 (2004).

[77] U.S. Department of State Bureau of Democracy, Human Rights and Labor, "Country Reports on Human Rights Practices – China, 2003, http://www.state.gov/g/drl/rls/hrrpt/2003/27768.htm, Section 2(a) para. 19 (visited 7/28/04)

[78] Qiu, Jack Linchuan, Virtual censorship in China: keeping the gate between the cyberspaces, 4 Int'l J. Comm. L. & Pol'y 1, 2 (1999/2000).

[79] House of Representatives Policy Statement, *supra* note 74 at ¶ 17.

[80] U.S. Department of State Bureau of Democracy, Human Rights and Labor, *supra* note 77 at para. 13.

in an electronic mail message.[82] In Vietnam, "politically … inappropriate" Internet content is blocked.[83]

(2) foreign influences

In China, the government demands and enforces strong control over content that can be made available via the Internet, blocking such foreign sources as the New York Times and CNN.[84] The Chinese government has blocked such Internet content as "sites of some major foreign news organizations, health organizations, educational institutions, Taiwanese and Tibetan businesses and organizations, religious and spiritual organizations, democracy activists, and sites discussing the June 4 Tiananmen massacre."[85]

French policymakers have viewed the international quality of the Internet as a potential challenge to France's cultural identity.[86] Consequently, the French government has promulgated guidelines and a policy framework that promote French culture, by approaches such as encouraging the use of French-language terms for the Internet[87] and requiring web pages in France to have substantial French-language content.[88]

Foreigners in Burma are prohibited from using private electronic mail and must have special authorization to bring electronic communication devices, such as modems, into Burma.[89]

(3) obscenity

In the United States, efforts to regulate obscene and indecent content on the Internet have met with roadblocks such as difficulties in balancing First Amendment interests with society's interest in controlling pornography.[90] Meanwhile, the quantity of pornographic websites, the

---

[81] House of Representatives Policy Statement, *supra* note 74 at ¶ 24.

[82] *Id.* at ¶ 30.

[83] *Id.* at ¶ 32.

[84] Solum, Lawrence B. and Chung, Minn, The layers principle: Internet architecture and the law, 79 Notre Dame L. Rev. 815, 897 (2004)

[85] U.S. Department of State Bureau of Democracy, Human Rights and Labor, *supra* note 77 at Section 2(a) para. 20.

[86] Preparing France's Entry into the Inform@tion Society: Government Action Programme at 7, cited in Smith, Pamela G., Free speech on the world wide web: a comparison between French and United States policy with a focus on UEJF v. Yahoo! Inc., 21 Penn St. Int'l L. Rev. 319, 330 (2003).

[87] *Id.*

[88] Eko, Lyombe, *supra* note 44 at 470.

[89] House of Representatives Policy Statement, *supra* note 74 at ¶ 24.

[90] Alexander, Mark C., The First Amendment and problems of political viability: the case of Internet pornography, 25 Harv. J.L. & Pub. Pol'y 977, 978 (2002)

number of visitors to those websites, and the revenue generated by those websites grow to substantial proportions of Internet usage.[91]

(4) child pornography

Sexual content involving children is illegal in most jurisdictions. The United States passed a federal statute to specifically address Internet transmission of child pornography,[92] including images that were created without the participation of children – which could mean that participants looked like minors but were not, and could also refer to virtual images produced by computer where no living persons were involved.[93] The U.S. Supreme Court found unconstitutional those provisions which did not protect actual children.[94] In response to the courts' decision, the U.S. Congress has introduced revised legislation (such as the Child Obscenity and Pornography Prevention Act, introduced in the House of Representatives last year[95]) in further attempts to prohibit this type of content.[96]

(5) sexually explicit content

In Saudi Arabia, non-pornographic but sexually explicit content – such as educational or medical materials – may be considered "immoral". The use of such "immoral" content has led the Saudi Arabian government to shut down some Internet cafés.[97]

(6) subversive materials

In China, use of the Internet to "incite the overthrow of the Government or the Socialist system" is expressly prohibited;[98] access is restricted and penalized for Internet content that is "subversive" or "critical" of the government;[99] and electronic mail messages containing "subversive" content are intercepted.[100] Laos blocks access to Internet content that is considered

---

[91] Magovern, Robert K., The expert agency and the public interest: why the Department of Justice should leave online obscenity to the FCC, 11 CommLaw Conspectus 327 (2003)

[92] Child Pornography Protection Act, 18 U.S.C. 2256(8).

[93] Child Pornography Protection Act, 18 U.S.C. 2256(8)(B) & 2256(8)(D).

[94] Ashcroft v. Free Speech Coalition, 122 S. Ct. 1389 (2002).

[95] Child Obscenity and Pornography Prevention Act, H.R. 1161, 108th Cong. (2d Sess. 2003).

[96] Marts, Jr., Gary D., First Amendment and freedom of speech – "It's OK – she's a pixel, not a pixie": the First Amendment protects virtual child pornography, Ashcroft v. Free Speech Coalition, 25 U. Ark. Little Rock L. Rev. 717, § V.C. (2003). *Also see* Krause, Jason, Can anyone stop Internet porn?, 88 A.B.A. J. at 56, 60 (Sept. 2002).

[97] House of Representatives Policy Statement, *supra* note 74 at ¶ 12.

[98] U.S. Department of State Bureau of Democracy, Human Rights and Labor, *supra* note 77 at Section 2(a) para. 22.

[99] House of Representatives Policy Statement, *supra* note 74 at ¶ 20.

[100] *Id.* at ¶ 26.

to contain "subversive information".[101] Saudi Arabia proscribes publishing or accessing material via the Internet that includes "subversive ideas."[102]

(7) proscribed activities

The State Council of China "has promulgated a comprehensive list of prohibited Internet activities, including using the Internet … to 'incite division of the country, harming national unification'",[103] to promote "evil cults", [104] and to make available information that "disturbs social order or undermines social stability" [105] A more recent revision of Internet regulations adds to the panoply of activities that are defined to be "subversion or slandering the state" ,[106] such as "dissemination of any information that might harm unification of the country or endanger national security". [107] The current set of Chinese Internet regulations are considered "so broadly written that MSS (Ministry of State Security) officials could find any Web page operator or e-commerce merchant guilty of violating regulations".[108]

In the United States, state and federal statutes make most Internet gambling illegal; obversely, at least fifty other national governments expressly allow Internet gambling in some form.[109] Some rationales for strict control of Internet gambling include concerns: that pathological gambling is a disease which is more likely to occur with the Internet's faster pace, increased privacy, longer hours of access, lower costs, and lack of "tangible representation of money", compared to physical casinos[110]; that Internet gambling would provide a breeding ground for fraud and money-laundering; and that underage gambling is encouraged by the availability of Internet gambling.[111]

---

[101] *Id.* at ¶ 19.

[102] Council of Ministers Resolution, Saudi Internet Rules, Feb. 12, 2001, Rule 7, http://www.al-bab.com/media/docs/saudi.htm (visited 7/28/04).

[103] U.S. Department of State Bureau of Democracy, Human Rights and Labor, *supra* note 77 at Section 2(a) para. 22

[104] *Id.* at Section 2(a) para. 21.

[105] *Id.* at Section 2(a) para. 21.

[106] *Id.* at para. 10.

[107] *Id.* at Section 2(a) para. 21.

[108] House of Representatives Policy Statement, *supra* note 74 at ¶ 26.

[109] Gottfried, Jonathan, The federal framework for Internet gambling, 10 Rich. J. L. & Tech. 26, I (2004).

[110] *See* Karadbil, Jenna F., Casinos of the next millennium: a look into the proposed ban on Internet gambling, 17 Ariz. J. Int'l & Comp. L. 413, 439 (2000).

[111] Gottfried, Jonathan, *supra* note 109 at III. A.-D..

(8) violation of public policy

Saudi Arabia disallows the use of the Internet for transmission of content "in violation of Islamic tradition."[112]

(9) infringing on rights of others

Some U.S. jurisdictions have promulgated regulations requiring filtering of sexual images on public library Internet terminals in order to protect employees from sexual harassment[113] and from a hostile work environment generated by sexual content viewed by library patrons,[114] in violation of the federal equal employment law.[115]

Existing common law and statutory law apply to Internet content that harms others, but often the application of these laws is stymied by the technological structure of the Internet: while the Internet's international reach and communication speed may exacerbate the harm,[116] the difficulty of tracing responsible parties confounds enforcement.[117] For example, traditional defamation law applies to Internet content that may harm a party's interests, but technical difficulties are faced when attempting to identify the creator of the content, because the Internet allows for virtual anonymity of its users,[118] although given sufficient resources and time, law enforcement observers conjecture that any Internet user can be tracked down.[119]

(10) harmful to minors

Where gambling via the Internet is regulated (such as in virtually all of the United States), one basis for this regulation is how vulnerable young people are to risky behavior and how the Internet may make gambling activities far more available and accessible to the young.[120]

---

[112] Internet Services Unit, Local Content Filtering Policy, para. 1, http://www.isu.net.sa/saudi-Internet/contenet-filtring/filtring-policy.htm (visited 7/28/04)

[113] Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library, 24 F. Supp. 2d 552, 556 (E.D. Va. 1998)

[114] Meehan, Kiera, Installation of Internet filters in public libraries: protection of children and staff vs. the First Amendment, 12 B.U. Pub. Int. L.J. 483, 497-98 (2003).

[115] Title VII, 42 U.S.C. 2000e-2e(a)(1) (2004).

[116] Zollers, Frances E., Shears, Peter, and Hurd, Sandra N., Fighting Internet Fraud: Old Scams, Old Laws, New Context, 20 Temp. Envtl. L. & Tech. J. 169, 171 (2002).

[117] *Id.* at 176.

[118] Goldring, Orit and Hamblin, Antonia L., Think before you click: online anonymity does not make defamation legal, 20 Hofstra Lab. L.J. 383, 386 (2003).

[119] Schwarz, Joel Michael, *supra* note 55 at 93.

[120] National Gambling Impact Study Commission, *National Gambling Impact Study Final Report*, at 1-1 (1999), at § 7-20 and § 7-24, http://govinfo.library.unt.edu/ngisc/reports/1.pdf (visited 9/13/04)

The United States has also attempted regulation of content specifically based on its being harmful to minors. The communications Decency Act of 1996 ("CDA")[121] prohibited transmission of "indecent" or "patently offensive" materials to minors.[122] The U.S. Supreme Court found the CDA to be an unconstitutional attempt to limit First Amendment[123] rights to free speech, principally because the terms "indecent" and "patently offensive" are "general, undefined terms" without a clear meaning.[124]

The U.S. Congress enacted the Child Online Protection Act ("COPA") to criminalize the knowing dissemination of material harmful to minors via the World Wide Web,[125] but COPA has not withstood Constitutional scrutiny by U.S. courts.[126]

More recently, the Children's Internet Protection Act ("CIPA") requires filtering technologies for all public schools and libraries with public computers, to prevent access to content that is "obscene" or "harmful to minors".[127] The U.S. Supreme Court upheld the constitutionality of CIPA, deciding that the statute does not violate library patrons' First Amendment rights.[128]

The U.S. Congress also recently enacted a statute to create a "Dot Kids" Internet second-level domain,[129] in which content is restricted by law to "only material that is suitable for minors and not harmful to minors."[130]

(11) racism, xenophobia

The Council of Europe's Additional Protocol on the Convention on Cybercrime defines racist and xenophobic content as "any representation of thought or theories, which advocates, promotes or incites hatred, discrimination or violence against any individual or group of individuals based on race, color, descent or national or ethnic origin."[131] This definition

---

[121] Communications Decency Act, 47 U.S.C. 223 (1996).

[122] *See id.* at 223(a) and 223(d).

[123] U.S. CONST. amend. I.

[124] Reno v. ACLU, 521 U.S. 844, 877 (1997).

[125] Child Online Protection Act, 47 U.S.C. § 231(a)(1) (2000).

[126] Ashcroft v. ACLU, 124 S. Ct. 2783 (U.S. 2004)

[127] Children's Internet Protection Act, 47 U.S.C. § 254(h)(5)(B) (2001).

[128] United States v. Am. Library Ass'n, 539 U.S. 194 (2003).

[129] *See* kids.us, http://www.kids.us (visited 9/13/04)

[130] Dot Kids Implementation and Efficiency Act, 47 U.S.C. § 941 (2002).

[131] Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems, opened for signature Jan. 28, 2003, Council of Europe

emphasizes the dangers to society of racist or xenophobic ideas, and supports initiatives to criminalize racist and xenophobic materials throughout the European Union.[132] Although Internet service providers are not liable for content that they do not create or control,[133] ISPs may be required by courts or administrative authorities to stop or prevent violations. [134]

In harmony with the European Union's approach to racist and xenophobic content on the Internet is Germany's restriction of such materials.[135] Germany's Penal Code criminalizes the publication and distribution of racist and xenophobic material,[136] and Germany's Multimedia Law extends the Penal Code's restrictions to the Internet.[137] Under Germany's Multimedia Law, Internet service providers (ISPs) are shielded from liability under clearly specified conditions, including the requirement that the ISPs block Internet material that is illegal in Germany.[138] Germany's highest court ruled that these laws apply to materials placed on the Internet from anywhere in the world, if the materials are accessible to Internet users in Germany.[139]

(12) incitement to illegal activities

Saudi Arabia specifically prohibits publishing or accessing via the Internet materials that are "liable to promote or incite crime" or is "slanderous or libellous … against individuals"[140]

(13) hate speech

The concept of hate speech goes further than racist or xenophobic speech, extending to speech against women, homosexuals, and other minorities.[141] In Canada, for example, the

---

T.S. No. 189, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&CL=ENG (visited 9/14/04).

[132] Proposal for a Council Framework Decision on combating racism and xenophobia, Eur. Parl. Doc. (COM 644 final) 6 (2001), http://europa.eu.int/eur-lex/en/com/pdf/2001/com2001_0664en01.pdf (visited 7/14/04).

[133] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, art. 12, § 4, 2000 O.J. (L 178), http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf (visited 7/14/04).

[134] *Id.*

[135] Timofeeva, Yulia A., Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany, 12 J. Transnat'l L. & Pol'y 253, 262-63 (2003).

[136] Strafgesetzbuch [Penal Code] §§ 130, 131.

[137] Mediendienstesstaatsvertrag [Media Law] § 12 abs.1.

[138] Mediendienstesstaatsvertrag [Media Law] § 9.

[139] Judgment of Dec. 12, 2000, Bundesgerichthof [Federal Court], regarding Frederick Toben and the website http://www.adelaideinstitute.org (visited 9/14/04)

[140] Council of Ministers Resolution, Saudi Internet Rules, Rule 9, Feb. 12, 2001, http://www.al-bab.com/media/docs/saudi.htm (visited 7/28/04).

[141] Weintraub-Reiter, Rachel, Hate speech over the Internet: a traditional constitutional analysis or a new cyber constitution?, 8 B.U. Pub. Int. L.J. 145, 149 (1998).

Canadian Human Rights Act prohibits repeated communication likely to expose one or more persons to "hatred or contempt" because of their "race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability, and conviction for which a pardon has been granted."[142] Canadian hate speech laws were amended in 2001 expressly to forbid "online hate propaganda" and the spread of "hate messages" by "all telecommunications technologies."[143] However, much of this speech may be legal in the United States.[144]

In the United States, most racist and xenophobic speech is protected under the First Amendment,[145] with exceptions for speech which is inherently dangerous[146] or injurious.[147] The possibility has been suggested that because United States allows speech that is illegal in other countries, the United States may become a "speech haven" for those whose speech would be prohibited elsewhere.[148] These conflicting laws can befuddle Internet service providers: for example, an Internet service provider, by removing a Nazi web site, may risk being sued in the United States for violation of First Amendment rights; by taking no action against a Nazi web site, may risk legal action in France or Germany.[149]

Some commentators point out that exceptions to First Amendment protection are particularly difficult to apply to Internet content, where most communication does not take place without the recipient taking deliberate steps[150], where most undesirable messages can be easily avoided, and where direct violence or injury is highly unlikely between sender and receiver of content.[151] Nevertheless, the Internet provides new tools for dissemination of hate speech, relatively inexpensively and highly effectively,[152] by facilitating establishment of special-interest

---

[142] Canadian Human Rights Act, R.S.C. 1985, c. H-6, s.3(1).

[143] Department of Justice Canada, Government of Canada introduces anti-terrorism act, Oct. 15, 2001, http://canada.justice.gc.ca/en/news/nr/2001/doc_27785.html (visited 9/15/04).

[144] Bailey, Jane, Private regulation and public policy: toward effective restriction of Internet hate propaganda, 49 McGill L.J. 59, 66 (2004).

[145] R.A.V. v. St. Paul, 505 U.S. 377 , 383 (1992).

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

[147] *See* Schenck v. United States, 249 U.S. 47, 52 (1919); Brandenburg v. Ohio, 395 U.S. 444 (1969).

[148] Brenner, Susan W., *supra* note 42 at 273.

[149] Goodman, Marc D., and Brenner, Susan W., The emerging consensus on criminal conduct in cyberspace, 2002 UCLA J. L. Tech. 3 § B (2002).

[150] Weintraub-Reiter, Rachel, *supra* note 141 at 165.

[151] Timofeeva, Yulia A., *supra* note 135 at 257-58.

[152] Proposal for a Council Framework Decision on combating racism and xenophobia, Eur. Parl. Doc. (COM 644 final) 6 (2001), http://europa.eu.int/eur-lex/en/com/pdf/2001/com2001_0664en01.pdf (visited 7/14/04).

groups, by accumulation of contact information for large audiences, both "potential followers and victims,"[153] and by virtually instantaneous distribution throughout the world.[154]

ii) Flow of information

(1) publishing

China provides an example of a government that asserts substantial control over dissemination of all forms of content, and perforce asserts this control over Internet content as well. Nevertheless, the Internet's technology makes such control challenging. In the case of advertising, China has no national act focused on Internet advertising, but rather covers all advertising under the Advertising Law of the People's Republic of China[155] – but the Internet makes it difficult to identify source and location of advertisements, and even whether particular content is an advertisement.[156] More clearly defined regulations in China control Internet publishing, which are directed at harmful content, and which expressly apply the current regulatory framework for physical publishing to Internet publishing.[157] Over 2,000 newspapers are published in China, with major papers providing Internet versions, all of which are subject to this regulatory structure.[158]

(2) private communication

Governments interested controlling Internet content are not limited to publicly accessible, published content such as websites. Private communications, such as electronic mail messages, can be subject to monitoring, scrutiny, censorship, and restriction as well. Some examples: The Cuban government controls all Internet access and is understood to censor all electronic mail messages.[159] Free electronic mail services are blocked in Syria.[160] In Burma, all electronic mail messages are screened by Myanmar Post and Telecommunications, and foreigners are prohibited

---

[153] Timofeeva, Yulia A., *supra* note 135 at 256-57.

[154] Rosenfeld, Michel, Hate speech in constitutional jurisprudence: a comparative analysis, 24 Cardozo L. Rev. 1523, 1524 (2003).

[155] Advertising Law of the People's Republic of China (1994), http://www.novexcn.com/advert_law_95.html (visited 9/14/04)

[156] Gao, Fuping, *supra* note 76 at 62.

[157] State Administration of Press and Publication and Ministry of Information Industry, Interim Regulations on the Administration of Internet Publishing (July 8, 2002).

[158] Keller, Perry, *supra* note 52 at 87.

[159] House of Representatives Policy Statement, *supra* note 74 at ¶ 8.

[160] *Id.* at ¶ 7.