The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question

Shamoil Shipchandler

Follow this and additional works at: http://scholarship.law.cornell.edu/cilj
Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.cornell.edu/cilj/vol33/iss2/4

This Note is brought to you for free and open access by Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell International Law Journal by an authorized administrator of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.
The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question

Shamoil Shipchandler*

I. Background
   A. History of the Internet
   B. How the Internet can be Regulated
      1. Regulation by Content
         a. Hardware Regulation
         b. Software Regulation
      2. Regulation by User Activity

II. Current Regulatory Attempts
   A. United States
   B. Germany
   C. China

III. Problems with Current Regulatory Attempts
   A. Practical Problems with Regulating the Internet
      1. Uniqueness of the Internet
      2. Jurisdiction over the Offender
      3. Enforcement of Regulations
      4. Policy Concerns
   B. Theoretical Problems with Regulating the Internet
      1. Private Regulation by Corporations
      2. Public Regulation by Nations
      3. Regulation by International Laws

IV. Non-Regulation as the Solution
   A. Concerns with Non-Regulation
      1. Objectionable Content
      2. Criminal Activity
      3. Sovereignty Concerns

* J.D., Cornell Law School, 2000; B.A., Middlebury College, 1996. Special thanks to my parents, Tamim and Farida Shipchandler, and my brother, Abeezaar, without whom none of this would be possible. A son could not ask for a more supportive family. Thanks also to R. Brian Black for his conscientious editing.
Introduction

In the 19th century, Americans in search of opportunity looked westward toward the Pacific Ocean. Settlers traveled the Oregon Trail finding a land unencumbered and uncluttered by excessive regulation: the "Wild West." Today's Wild West is the Internet. Instead of the Oregon Trail we have the electronic superhighway.

Limitless opportunities abound on the Internet, and the laissez-faire freedom of electronic transactions hastens the development and growth of the Internet. Currently, an estimated three hundred million people use the Internet worldwide. These electronic settlers are a force that nations seek to control, but cyberspace is a vacuum that abhors regulation.

Because of this regulatory vacuum, nations fear the Internet, for while the Internet harbors enormous potential for access to information, it also poses a threat to state sovereignty and traditional state boundaries. Nations and governments cannot effectively regulate that which has no boundaries and no physical presence, can disseminate information globally in an instant, and seemingly exits everywhere, yet is located nowhere.

Nations seek to fence in the Internet using rules and regulations. Nevertheless, governments bent on regulating the Internet face several practical problems. With whom does one negotiate? Who is paying attention to the government's requests? Who will heed? Who really owns the Internet? At least one group has expressed a desire for absolute Internet independence, pronouncing the Declaration of the Independence of Cyberspace:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave me alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

3. Cyberspace is synonymous with the Internet.
The drive of nations to regulate the Internet and the natural tendency of the Internet to frustrate such efforts is the focus of this Note, which argues that nations should not attempt to regulate the Internet until the medium stabilizes. Neither private nor public Internet regulation is effective at this time, and Internet users can and probably will regulate themselves, especially when provided the proper incentive. This Note does not argue that non-regulation of the Internet is beneficial, nor does it attempt to identify all Internet content as acceptable. It merely analyzes and critiques the regulatory attempts currently employed by leading nations and adopts a "wait and see" approach.

Part I provides background information about the Internet and describes the available methods of regulation. Part II discusses current regulatory attempts by the leading nations in Internet use: the United States, Germany, and China. Part III explores the difficulties in regulating the Internet, focusing on how these nations' attempts at regulation have failed. Part IV demonstrates that in the face of its evolving technology and global reach, the Internet should be left unregulated for now.

I. Background

A. History of the Internet

Nations seeking to regulate Internet activity must understand the Internet's origins and the technology involved. By design, the Internet's infrastructure is not centralized in any one location, but rather dispersed globally. The Internet's origin and the circumstances of its development are sources of difficulty for nations in conceptualizing and regulating the electronic superhighway.

In 1958, President Eisenhower and the Department of Defense founded the Advanced Research Projects Agency (ARPA) to unite the United States' highest levels of research, protect U.S. communications from catastrophic nuclear attack, and minimize computing costs. ARPA adopted a "distributed network" model, which means the network would connect stand-alone computers to each other and use them as a group, instead of concentrating computing power in a single machine. Further-
more, on a distributed network model, attacking one computer would do little damage, if any, to the overall network. Finally, to improve the security of electronic mail (e-mail) and other transmissions sent over the network, ARPA used packet switching, which allowed network messages to be broken into smaller components (packets) and transmitted piecemeal to their destination.

By 1969, the government had installed ARPA's network at four locations: the University of California at Los Angeles, Stanford University, the University of California at Santa Barbara, and the University of Utah. Later installations followed at the Massachusetts Institute of Technology, Harvard University, Case Western Reserve University, and Carnegie Mellon University. Initially, researchers at these institutions used the network to facilitate communication with each other.

In 1972, the wealth of information available on ARPA's network expanded significantly with the creation of the Transmission Control Protocol/Internet Protocol (TCP/IP). While the Internet formerly transmitted communications only by writing and re-writing to the network, TCP/IP allowed the exchange of data without modifying the network. Furthermore, TCP/IP enabled each computer to find other networked computers via global addressing, using numbers, not geographic location, to denote network addresses. With these refinements, e-mail became the most popular use for the network.

The next major change for ARPA's network occurred in 1989. Tim Berners-Lee, a researcher at the CERN atomic research center in Switzerland, proposed a set of software commands that established a user-friendly "point-and-click" system for browsing documents. This new set of com-

58-59. However, since a central hub for the entire network would be vulnerable to attack, ARPA adopted the distributed network model. See Geist, supra note 9, at 527.
11. See Geist, supra note 9, at 527.
12. See HAFNER & LYON, supra note 6, at 59-61. The recipient's computer would reassemble the packets into a coherent whole. See id. This process enabled secure messaging by prohibiting the interception of a complete message at any midpoint on the network. See id.
14. See HAFNER & LYON, supra note 6, at 166.
16. See id. at The Initial Internettig Concepts.
17. See id. Writing and re-writing to the network is a laborious process, where a computer would copy a message to the network and the recipient computer would download it. Exchanging data between computers directly revolutionized message delivery. See id.
18. See id.
19. See HAFNER & LYON, supra note 6, at 194. An ARPA study found that in 1973, roughly seventy-five percent of network use was e-mail. See id. Still the most common use of the Internet, forty million people have sent e-mail as of 1995. See Fixler, supra note 7, at 83.
mands developed into Hyper-Text Markup Language (HTML).\textsuperscript{21} Most importantly, this language used "hyper-links" that would automatically "jump" users to a new location when selected.\textsuperscript{22}

Researchers further refined Berners-Lee's innovation in 1993 by improving Internet users' software and simplifying the browsing experience.\textsuperscript{23} While most early browsers were primitive and unstable, advancements in the understanding of HTML inspired Marc Andreeson at the National Center for Supercomputing Applications (NCSA) to create the Mosaic browser.\textsuperscript{24} Using a graphical interface, Mosaic allowed users to visually survey Internet sites.\textsuperscript{25} Further refinements led to fairly sophisticated programs like Netscape's Communicator and Microsoft's Internet Explorer.

Today's Internet still reflects characteristics of the original ARPA network; interconnected stand-alone computers give the appearance of a web, hence the term "World Wide Web." There are currently an estimated three hundred million Internet users worldwide.\textsuperscript{26} As of April 1995, there were approximately 23,000 web sites on the Internet.\textsuperscript{27} With the number of new users roughly doubling every one and a half years, the Internet's growth is astounding.\textsuperscript{28}

The rapidly growing size and widely-dispersed nature of the Internet explain the challenges in regulation. Nations considering Internet regulation must examine the changing technology and predict future evolution. Static regulation will quickly be outdated as the Internet changes. Furthermore, the threat of regulation resembles a nuclear attack — a threat that motivated ARPA to use a distributed information system for the Internet that could not easily be compromised or shut down.\textsuperscript{29} Similar to a physical threat, national regulation would attack only one geographical portion of the Internet. However, due to the Internet's distributed nature, such attack would have little effect on the Internet as a whole.

B. How the Internet can be Regulated

At a technical level, nations only have two options for actively regulating the Internet. First, the government can regulate the content of web

\textsuperscript{22} See Weintraut, supra note 20, at xxii-xxiv.
\textsuperscript{23} See id. at xxv.
\textsuperscript{24} See id.
\textsuperscript{25} See id.
\textsuperscript{26} See Nua Survey, supra note 2.
\textsuperscript{27} See Russell B. Stevenson, Jr., Internet Payment Systems and the Cybercash Approach, 452 PLI/Pat 123, 127-28 (1996).
\textsuperscript{29} See supra notes 7, 11 and accompanying text.
sites. Second, the government can regulate user activity by controlling citizens' access to the Internet.

1. Regulation by Content

Due to the sheer breadth and scope of the Internet, true content regulation by nations is extremely difficult, if not impossible. Nations can filter the content of web sites in two ways: hardware regulation and software regulation. However, both methods suffer from inherent flaws.

a. Hardware Regulation

The information on the Internet is intangible and electronic; thus, in a technical sense, impossible to regulate. However, instead of regulating the information, regulations can seek to control the physical tools used to access information. A nation's easiest response is to have nothing to do with the Internet, technological isolation, foregoing all possible benefits of connectivity. Although a radical solution, as of July 1996, thirty-three countries had chosen this option. Alternatively, nations can create a hierarchical network and force outside Internet activity through a gateway before allowing citizens to access it. The government could maintain and regulate the gateway directly or regulate the Internet Service Providers (ISPs) that provide access to the Internet. Unfortunately, these solutions would not be completely effective. Users could avoid gateway restrictions simply by dialing into a "pure" ISP for an unregulated feed to the Internet. However, this avoidance tech-

31. See Wu, supra note 30, at 655-56.
33. See Wu, supra note 30, at 651-55.
34. "Physical tools" refers to the tangible machinery used for Internet access. The phrase include servers, computers, monitors, keyboards, etc.
35. See, e.g., Not Too Modern, Please: Asia and the Internet, THE ECONOMIST, Mar. 16, 1996, at 42, available in 1996 WL 8671264 (discussing Asian countries' desire for the fruits of connectivity, but also their concurrent wish to regulate it).
36. See Wu, supra note 30, at 651.
37. See id.
38. Conceptually, a gateway works like a funnel. All Internet information enters the top of the funnel. As information flows through the funnel, the government removes any information it does not want citizens to receive, which could include shutting off the flow of information entirely. Thus, information emerges regulated at the bottom of the funnel.
39. See infra Part II.C (discussing China's Intranet).
40. Most users pay ISPs an hourly or monthly fee for access to the Internet. Access is most commonly provided through telephone lines, but recent technological developments have allowed access through the cable television infrastructure and direct Ethernet connections to the Internet's infrastructure.
41. See infra Parts II.B-C (discussing ISP liability in Germany and China).
42. See Wu, supra note 30, at 652. Ostensibly, a pure ISP could be found in a country with fewer content restrictions.
nique is costly, and few citizens would have the requisite resources.  

b. Software Regulation

Instead of choosing to regulate the Internet through restrictive hardware, nations could regulate through software. Software regulation could be imposed at two stages: regulation at the router level and regulation at the end-user level. To regulate at the router level, nations can establish a "firewall" which filters out any unwanted sites or information. Using this firewall, a government could prevent users from accessing all information outside the firewall, except for government-approved sites. China, for example, uses a firewall on a nationwide scale to protect and insulate data from the rest of the Internet.

To regulate at the end-user level, a nation could filter the Internet through the user's browser. The nation would need a rating system for Internet sites. One example is the Platform for Internet Content Selection (PICS). If web sites broadly adopted this protocol, any PICS-rated browser would screen out inappropriate sites based on the rating. If a government only permitted use of PICS-compatible browsers, that nation could define undesirable content before allowing the end-user to access information.

However, this system is not perfect. Users could avoid browsers that screen objectionable sites, and "pirated browsers [without a screening mechanism] would likely proliferate." Also, the system relies on web sites to use the rating system accurately.

---

43. See id.
44. See id. at 652-55.
45. See id.
46. See id. The router level is the mediate stage between the sender and recipient where information crosses the Internet. The end-user level is the final stage where the user downloads information from the Internet.
47. To conceptualize a firewall, think of a medieval castle and moat. The moat protects the castle; with the drawbridge up, the moat restricts all access to the castle. When the drawbridge is down, castle access is limited. A monarch regulates castle access by controlling the drawbridge. In this example, the moat is a firewall, the outside world is the Internet, and the castle and its contents are called an "Intranet." The drawbridge would be the ISP that connects the Intranet and Internet. See John Wack & Lisa Carnahan, Keeping your Site Comfortably Secure: An Introduction to Internet Firewalls (posted Feb. 9, 1995) <http://csrc.ncsl.nist.gov/nistpubs/800-10/> (National Inst. of Standards & Tech. Special Publication No. 800-10).
48. See infra Part II.C. Many U.S. corporations use a firewall to protect data within the company. See generally Wack & Carnahan, supra note 47.
49. See Wu, supra note 30, at 653.
51. See Wu, supra note 30, at 653.
52. See id. at 654.
53. Id.
54. See Weinberg, supra note 50, at 470.
2. Regulation by User Activity

Regulation by content places the onus on the government to identify information that citizens ought not see. After this initial designation, the government can shield citizens by making access to undesirable sites impossible. With this relatively heavy-handed approach, however, the nation makes moral judgments for its citizens.55

On the other hand, regulation by user activity allows the government to exercise power more judiciously. Instead of technological solutions, regulation by user activity involves punishing behavior.56 For example, instead of mandating that all browsers bar access to pornographic web sites, the nation could enact legislation criminalizing the creation and/or uploading57 of such web sites.58

There are benefits to this approach. Regulating by user activity simplifies jurisdictional concerns. For example, regulations need not consider the location of an undesirable web site's owner. If the web site's owner resides in Germany, China, or elsewhere, a government would still retain personal jurisdiction over the individual downloading the undesirable material.

Nevertheless, this type of regulation fails to have a substantial impact on individuals' conduct because the broad and decentralized nature of the Internet makes enforcement difficult.59 Officials have considerable difficulty locating individuals that access illegal web sites. Due to the relatively cheap cost of using the Internet,60 every individual is a possible offender. Therefore, while being the least intrusive into cyberspace, regulation by user activity is also the least effective at obtaining results.

II. Current Regulatory Attempts

Many nations are only now investigating how best to cope with the new technology of the Internet. Since the Internet has no geographical

55. A more tangible example of content regulation is banning books based on their content. The government makes an initial determination of appropriate material for citizens to read and bans all inappropriate books.


57. Uploading refers to copying files to a server so that any Internet user may access them. In contrast, downloading refers to copying files from the Internet to a local computer.

58. As a more specific example, the United States has neither mandated modification of browsers to skip child pornography sites nor created a gateway to sift through sites before offering them to its citizens. Instead, the United States makes it illegal to upload child pornography to the World Wide Web. See, e.g., Child Pornography Protection Act of 1996, Pub. L. No. 104-208, § 121, 110 Stat. 3009, 3009-26 (enlarging the definition of child pornography and incorporating computer-generated images of child pornography within the scope of the statute).

59. See Johnson & Post, supra note 32, at 1370-76. But see Wu, supra note 30, at 655-56.

boundaries, national regulations have a profound international impact. With over three hundred million people in approximately 146 nations accessing the Internet, national regulation is impractical, inconsistent, and nearly impossible. While many nations are just beginning to understand the effect of the Internet, the world's leading nations have sought to control Internet content or, at the very least, access to the Internet. The United States and China have established some of the most advanced regulatory regimes, while Germany has struggled with its own Internet dilemmas. This section will explore the regulatory efforts in these nations for the later purpose of analyzing why those efforts have failed.

A. The United States

The United States prides itself on its Constitution where freedom of expression plays a primary role in ensuring democracy. According to the Constitution, freedom of expression, manifests itself through free speech, freedom of association, and freedom of religion. These basic principles are implicated by activities on the Internet. Unfortunately, the United States has little or no clear conception of how to reconcile constitutional freedoms with Internet use. For example, the United States primarily has targeted pornography as the greatest threat on the Internet. However, since pornography strongly implicates the First Amendment, it is also the cornerstone for U.S. difficulties in regulating the Internet. One of the first nations to pass legislation governing Internet use, the United States Congress passed the Communications Decency Act of 1996 (CDA).

For example, the United States primarily has targeted pornography as the greatest threat on the Internet. However, since pornography strongly implicates the First Amendment, it is also the cornerstone for U.S. difficulties in regulating the Internet. One of the first nations to pass legislation governing Internet use, the United States Congress passed the Communications Decency Act of 1996 (CDA).

62. See Nua Survey, supra note 2.
63. See Delacourt, supra note 61, at 207.
65. See U.S. Const. amend. 1.
67. See id.
68. See 47 U.S.C. § 223(a)-(h). The CDA was included as Title V of the Federal Telecommunications Act, which focused predominantly on reducing regulation and promoting competition in local telephone and broadcast markets. See 47 U.S.C. § 223; see also ACLU, 521 U.S. at 857-58.
69. The CDA barred the use of any telecommunications device to create or solicit any "indecent" message. In addition, the CDA criminalized the use of an interactive computer service to send minors any communication that would be patently offensive under contemporary community standards, make such communications available to minors, or intentionally allow telecommunications to be used for such a purpose. See 47 U.S.C. § 223(a)(1)(B), (d)(1)-(2).
that sought to limit access by underage individuals. The United States' efforts to limit ISP liability contrast sharply with efforts of China and Germany to impose liability on ISPs.

Yet, criticism leveled at the CDA argued that simple legislation was not fluid enough to cope with the rapidly changing Internet. Congress would be "unable to keep up with the frequent shifts in communications technology and the resulting shifts in federal jurisprudence." Also, immediately after the CDA's passage, twenty plaintiffs and the American Civil Liberties Union (ACLU) challenged two provisions of the CDA as unconstitutional violations of the First Amendment and the Due Process Clause of the Fifth Amendment. Upon review by the Supreme Court, the majority in Reno v. ACLU found the CDA's terms, "indecent" and "patently offensive," unconstitutionally overbroad and vague. While the Court rejected the CDA provisions related to indecent and patently offensive language, no parties challenged the CDA provisions restricting child pornography or obscenity.

However, the United States has attempted other means of regulation, most notably voluntary regulation by content through software programs. Designed to restrict access to web sites with objectionable content, one example of a content-based self-regulatory program is CyberPatrol. CyberPatrol and similar programs maintain a list of web sites with objectionable content. Once activated, CyberPatrol prevents the user from accessing sites on the list. Designed to shield children from objectionable content, CyberPatrol has been used extensively in Boston, where Mayor Thomas Menino and the Boston Public Library installed the program on all computers available to minors. Unfortunately, CyberPatrol and similar programs tend toward overbroad application, inexplicably restricting some web sites.

Some ISPs, like America Online, also include parental controls that

---

70. See 47 U.S.C. § 223(c). This provision protected corporations that attempted to screen out underage users using age verification techniques, most commonly by requiring credit card numbers. See, e.g., Adult Check, Adult Check: Webmaster Info (visited Apr. 22, 2000) <http://www.adultcheck.com/cgi-bin/merchant.cgi?9999>.

71. See infra Parts II.B-C.


73. Id.


75. See id. at 864.

76. See ACLU, 521 U.S. at 883.

77. See Weinberg, supra note 50, at 477-82; see also supra Part I.B.1.b.


80. See id.

81. See id.

82. See Mason, supra note 78, at 29.
allow parents to block their children's access to certain sites. These controls rely on the existence of certain words in a web site to activate the block. Unfortunately, this mechanism too can be overbroad. Words like "sex" or "breast" may trigger the control software, but "[w]hat you get is a system that ends up blocking information on breast cancer and Middlesex, England."

B. Germany

Germany and the United States share a similar ideological and regulatory response to the Internet. Both countries have constitutional provisions that guarantee free speech, but restrict some forms of expression, like obscenity. Germany also regulates hate speech, as demonstrated by its reaction to pro-Nazi propaganda on the Internet. Nevertheless, unlike the United States, Germany has relied on threats of prosecution against ISPs to force self-regulation.

Germany's first confrontation with the Internet occurred in December 1995, when the Bavarian Justice Ministry discovered online discussion groups that contained objectionable material. The Ministry notified CompuServe, a U.S.-based ISP, and threatened prosecution, including prison terms for company officials, if the groups were not blocked from German access. The threat of prison terms for senior company officials persuaded CompuServe to block access. However, since CompuServe's technology could not provide differentiated blocking, the threat forced CompuServe to block access for not only the 200,000 German subscribers, but also its other four million customers in 147 countries.

Examined closely, the German government's threat demonstrated its commitment to holding ISPs responsible for Internet content. Accordingly, Germany tacitly rejected screening software as a viable means of regulating the Internet. Instead, the German government takes the moral high ground, identifying objectionable content for the user. Thus, Internet users are not "responsible for protecting their own sensibilities." In addition, by threat-

---

83. See Michael Meyer, A Bad Dream Comes True in Cyberspace, NEWSWEEK, Jan. 8, 1996, at 65.
84. See Mason, supra note 78, at 29.
85. See id.
86. See Delacourt, supra note 61, at 208-15.
87. See Patrick G. Crago, Fundamental Rights on the Infobahn: Regulating the Delivery of Internet Related Services Within the European Union, 20 HASTINGS INT'L & COMP. L. Rev. 467, 484-85 (1997); see also infra notes 96-100 and accompanying text.
88. See Delacourt, supra note 61, at 212-13.
89. See Nathaniel Nash, Holding Compuserve Responsible, N.Y. TIMES, Jan. 15, 1996, at D4 (describing Germany's confrontation with CompuServe and the ISP's subsequent concessions).
90. See id.
91. See id.
92. See Meyer, supra note 83, at 65.
94. Delacourt, supra note 61, at 213.
ening German prosecution, Germany imposed this morality on other nations since CompuServe restricted access to the objectionable groups for all of its users.  

German officials confronted objectionable content again when they discovered neo-Nazi publications on the web. German prosecutors informed three ISPs that they faced liability for publishing these works. T-Online, a German ISP owned by Deutsche Telekom, immediately restricted access to the objectionable sites, but also cut off access to more than 1500 innocent sites. The other two ISPs, U.S.-based America Online and CompuServe, refused to restrict access to the sites. In addition, private "anti-censorship advocates at several United States universities engaged in efforts to thwart the restrictive actions of T-Online" by creating mirrors of the objectionable sites. The prosecutor, rationalizing his attempts to identify objectionable content on the Internet as a German crime, argued, "because [the neo-Nazi material is] available over the Internet, it also can be called up in Germany . . . [t]hen the scene of the crime is all of Germany."  

T-Online admitted that restricting access to 1500 innocent sites was not effective. Nonetheless, the desire to escape liability drove it to take strong measures to ensure compliance with German authorities. The German government prosecuted a CompuServe executive for distribution of pornography and Nazi propaganda, but the Bavarian High Court reversed the conviction. While the case was pending, the German government enacted the Information and Communications Services Act, which sets ISP liability standards for allowing distribution of objectionable material.  

Germany's response to Internet regulation indicates a dilemma similar to that of the United States. Both countries share a moral repugnance for certain types of expression and have attempted to stop its distribution on the Internet. The criminalization of user conduct or ISP liability, however, proved ineffective in neutralizing Internet distribution.

95. CompuServe blocked access to the "alt.sex" discussion group hierarchy. See Knoll, supra note 93, at 287.
96. See Delacourt, supra note 61, at 213. The works were written by Ernst Zundel, a Toronto-based neo-Nazi, and the Institute for Historical Review, a California-based organization publishing Holocaust denial literature. See id.
97. See Knoll, supra note 93, at 288. One example of an "innocent" site was Deutsche Bank Securities. See id.
98. See Delacourt, supra note 61, at 214.
99. Id. Mirror sites are duplicates of web sites, stored on the Internet independent of the original. So, if a site has been restricted, an exact copy of the restricted content would be available on the mirror site.
101. See Knoll, supra note 93, at 288.
102. See id. at 288-89.
C. China

While the United States and Germany struggle to reconcile Internet regulation with the basic freedoms granted to their citizens, China operates in a political atmosphere where no such guarantees exist. Thus, China gravitates toward draconian Internet regulation, and Chinese officials use a heavy hand in determining what content is appropriate for public exposure. On the positive side, China "seems to have a clear vision of how development and use of the Internet should proceed. . . . China's simple, yet extremely ambitious goal, can be described most succinctly as 'eliminat[ing] what is undesirable and keep[ing] what is good.' While this is a rather vague goal by Western standards, China's political ideology gives it powerful effect.

China conceptualizes the Internet as a tool for economic growth and nothing more. Unlike Western countries, China is not especially concerned with protecting speech, whether "regular" or on the Internet. Accordingly, China approaches Internet regulation differently from its Western counterparts. In China, the government identifies desirable content. "Unlike the United States and Germany, which look to the vast content of the Internet and ask what should be blocked, China asks what should not be blocked." The government can and does prohibit most web content beyond that used for normal business purposes. Even if not prohibited outright, China affords web sites no particular legal freedom, allowing "several layers of governmental jurisdiction over Internet control."

China endorsed its Internet Management Rules (Rules) during the forty-second meeting of the State Council on January 23, 1996. Subsequently, China's Premier Li Peng signed the Rules into law. The Rules describe the two methods China will use to control Internet content: first, the Chinese government prohibits unregistered use of and unrestricted content from the Internet, and second, the government limited physical

106. See Feir, supra note 105, at 376-82.
107. See Delacourt, supra note 61, at 215 (brackets in original) (citing Joseph Khan et al., Chinese Firewall: Beijing Seeks to Build Version of the Internet that can be Censored: Crackdown on Outside Views also Includes Satellite TV and Financial News Wires, WALL ST. J., Jan. 31, 1996, at A1 (quoting James Chu, "a Hong Kong computer scientist working with the Chinese government' on China's Intranet)).
108. See id.; Knoll, supra note 93, at 297.
110. See Delacourt, supra note 61, at 215.
111. Id.
112. See id. at 633-36.
113. Feir, supra note 105, at 368.
114. See Text of Interim Internet Management Rules, supra note 64.
115. See Feir, supra note 105, at 368.
116. See id.
access to the Internet.\textsuperscript{117}

Technically, the Chinese system routes the Internet through two government-controlled gateways.\textsuperscript{118} Then, firewall technology\textsuperscript{119} restricts links to the outside World Wide Web and basically creates China's national Intranet.\textsuperscript{120} With its own Intranet, China's firewall functions as a barrier so information cannot flow in or out, effectively creating a "digital Great Wall of China."\textsuperscript{121} Thus, Chinese ISPs provide access to the Chinese Intranet, as opposed to the global Internet.\textsuperscript{122} The additional prohibitions on unregistered use of and content from the Internet demonstrate China's commitment to censorship. By controlling what citizens can upload to the Internet, the government seeks to perpetuate the strict political controls already in place.

Following promulgation of the Rules, the government reduced network access to the Internet by forcing ISPs for the Intranet to use only those Internet feeds approved by China's Ministry of Posts and Telecommunications.\textsuperscript{123} In August 1996, the government took a more drastic step by blocking access to approximately one hundred web sites on the Internet that Chinese officials "suspected of carrying spiritual pollution."\textsuperscript{124} The restricted sites included many with information about Taiwan and Hong Kong, pornography, and U.S. media coverage.\textsuperscript{125} Finally, the government ordered Chinese ISPs to self-regulate and restrict all objectionable content accessible by their customers.\textsuperscript{126} Compliance with this regulation facilitates the Chinese government's efforts to monitor and censor Internet sites.\textsuperscript{127}

III. Problems with Current Regulatory Attempts

Although the United States, Germany, and China have taken steps to regulate the Internet, all have had difficulty obtaining desired results. This section will first examine the practical reasons for these difficulties, mostly dealing with how the Internet's structure complicates any form of localized, territorial attack. Then, it will explore the theoretical problems that nations have yet to confront or solve, focusing on the choice as to who

\begin{itemize}
\end{itemize}
regulates the Internet: private companies,\textsuperscript{128} nations themselves,\textsuperscript{129} or international treaties.\textsuperscript{130}

A. Practical Problems with Regulating the Internet

Nations have great difficulty regulating the Internet because of its global nature. Any attempt at regulation remains limited to the nation’s territorial boundaries. Thus, nations have several practical problems: (1) the Internet's uniqueness;\textsuperscript{131} (2) jurisdiction over offenders;\textsuperscript{132} (3) enforcement of regulations; and (4) policy concerns with regulation.

1. Uniqueness of the Internet

The Internet’s uniqueness places nations on unfamiliar ground, posing difficulty for regulatory attempts. The Internet is a unique communications medium and technology.\textsuperscript{133} The Internet outstrips most other communications media in terms of cost, speed, and power to disseminate information.\textsuperscript{134} Among the new forms of communication used on the Internet are e-mail and newsgroups.\textsuperscript{135}

E-mail is the most frequently used function on the Internet.\textsuperscript{136} With e-mail, “[m]essages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another.”\textsuperscript{137} In addition, unlike regular mail, the cost and speed of e-mail are unrelated to the distance a message must travel.\textsuperscript{138} This easy and instantaneous delivery leads to great difficulty restricting the flow of information across the Internet.

Although less popular than e-mail, newsgroups allow users worldwide to post and view messages, akin to a physical bulletin board.\textsuperscript{139} In this fashion, a posted message quickly reaches thousands of Internet users.\textsuperscript{140} Using newsgroups, “a person can act like a broadcaster; he can quickly and

\begin{itemize}
  \item \textsuperscript{128} See supra Parts II.B-C (discussing German and Chinese attempts to hold ISPs liable for Internet content).
  \item \textsuperscript{129} See supra Parts II.A-B (discussing U.S. and German attempts to legislate against objectionable content).
  \item \textsuperscript{132} See generally Stephan Wilske & Teresa Schiller, \textit{International Jurisdiction in Cyberspace: Which States May Regulate the Internet?}, 50 FED. COMM. L.J. 117 (1997).
  \item \textsuperscript{133} See Sato, supra note 130, at 707-10.
  \item \textsuperscript{134} See id.
  \item \textsuperscript{135} See id.
  \item \textsuperscript{136} See HAFNER & LYON, supra note 6, at 194.
  \item \textsuperscript{137} Johnson & Post, supra note 32, at 1370-71.
  \item \textsuperscript{138} See id.
  \item \textsuperscript{139} See Sato, supra note 130, at 708-09.
  \item \textsuperscript{140} See id.
\end{itemize}
easily disseminate a message to a large audience.\textsuperscript{141} Thus, as Germany discovered,\textsuperscript{142} it is difficult to control information originating from the Internet.

The Internet's predecessors, satellite television, radio, and telephone, presently offer the same global capability as the Internet, but are still comparatively easy to regulate.\textsuperscript{143} For example, unlike radio transmission,\textsuperscript{144} the Internet cannot be jammed.

The Internet also derives its uniqueness as a communications medium from its ease of access and low barriers to broadcasting.\textsuperscript{145} The physical tools required to connect to the Internet, are relatively inexpensive, consisting of a simple stand-alone computer and phone line.\textsuperscript{146}

The most important differentiating characteristic of the Internet is its extremely low barriers to entry. Because it uses other underlying physical communications infrastructures, a new Internet enterprise need not build a radio transmitter, string wire, or lay cable. All it takes to be an Internet publisher is a $2,000 personal computer and a $12.95 per month subscription to an Internet service provider. All it takes to be an Internet service provider is about $50,000, most of which goes for labor costs and a high bandwidth connection between the terminal server and router into the larger Internet. This is far less than what it takes to become a radio broadcaster, a print publisher or a telephone service . . . .\textsuperscript{147}

Low barriers to entry pose a particular problem for China, which seeks to regulate the Internet by controlling all points of entry into the country and filtering Internet content through its ministries.\textsuperscript{148} Citizens can avoid China's Intranet controls by making a simple long-distance phone call to an outside ISP; thereby receiving unfettered access to the Internet.\textsuperscript{149} China counteracts this difficulty not through technological barriers but intimidation of its citizens.\textsuperscript{150}

The low barrier to entry does not, however, fully explain the difficulties in Internet regulation. The Internet's unique technology renders nations' regulations modeled after satellite and telephone technology inapplicable and ineffective. The varying experiences of the United States, Germany, and China reflect the problems inherent in these technological differences.

The United States encountered difficulties treating the Internet as an extension of the telephone or press, cable, or radio medium.\textsuperscript{151} Attempting to impose content guidelines pertaining to indecency, the United States'
actions met with disapproval and rejection by the Supreme Court. The Court recognized the Internet as a new technology, not subject to similar limitations found in other communications media. The Supreme Court's distinctions between various forms of communication make it difficult for the United States to legislate all media as a whole.

Germany falls between the United States and China with regards to treatment of the Internet as new technology. So far, Germany has used existing laws to control Internet content. After the CompuServe incident, however, Germany became the first Western democracy to indict and convict an ISP executive for content the government deemed illegal. Also, the German government enacted the Information and Communications Services Act, which set standards for Internet content uploaded or downloaded to computers within German borders. Germany's end result has left it in the same predicament as the United States: effective legislation is hampered by differences in technology.

China, on the other hand, has carefully avoided treating the Internet like other technologies. Recognizing the inherent dangers of the Internet as a medium for free speech, China has attempted to enforce strict controls governing use. "[T]he Chinese government has been encouraging access to what is often an anarchic bastion of free expression and free flowing information, concurrent efforts to restrict and regulate the flow of information demonstrate the government's desire to maintain control." Whether these controls are working is debatable, but most critics agree that the regulatory efforts in China will fail eventually.

2. Jurisdiction over the Offender

Jurisdiction and enforcement are entwined, and both are sources of concern for nations attempting to regulate the Internet. A major issue in Internet jurisdiction is determining whether a nation has the right to prosecute an offender who resides in one nation and complies with that nation's laws, but violates another nation's laws because of the Internet's global reach. For example, if a U.S. citizen posts on the Internet material permitted by the CDA but deemed illegal in China, the issue becomes whether the individual is subject to Chinese prosecution.

153. See id.
154. See supra Part II.B. (discussing Germany's efforts to hold CompuServe, America Online, and T-Online responsible for violating hate speech laws).
155. See Dennis, supra note 103 (noting the CompuServe executive's subsequent acquittal by an appellate court).
156. See Dennis, supra note 104.
157. See Taylor, supra note 105, at 631-37 (explaining Chinese efforts to promote Internet use while regulating content).
158. See id at 630.
159. Id. (footnote omitted).
160. See id. at 637-39.
161. See Wilske & Schiller, supra note 131, at 125.
The United States, in addition to holding corporations liable for certain material uploaded to the Internet, evades the jurisdictional issue by holding its citizens responsible for what they post or download from the Internet. Although this approach gives the United States more leeway in prosecuting offenders, it leaves fewer offenders to prosecute. The Internet's relative anonymity exacerbates this limitation due to the difficulty authorities have tracking down offenders.

In its confrontation with CompuServe, Germany also had difficulty tracking down offenders. However, Germany encountered additional problems when it attempted to hold CompuServe liable for users' wrongdoing. Assuming German laws allowed the prosecution of any individuals uploading Nazi propaganda to the Internet, Germany had subject-matter jurisdiction over the user, a U.S. citizen. Unfortunately, even if it had jurisdiction, Germany had no way of enforcing its authority because, as a U.S. citizen, the user was protected by the First Amendment of the U.S. Constitution. "The United States is hesitant to support extradition in view of the United States citizens First Amendment rights, whereas the German government desires to prosecute the United States citizen under German law." Jurisdiction in Germany matters little, since there is no way for Germany to enforce its interest.

China's approach appears to be a combination of U.S. and German laws, but with a twist. In China, the user and ISP share liability for improper content on the Internet. Nevertheless, it is not liability that effectively chills Internet content, but the fact that "to the extent that the Chinese government can frighten its people, they will succeed in their control." Although hampered by the same problems that the United States and Germany encounter with extraterritorial jurisdiction, China may frighten users and ISPs into compliance with regulations for its Intranet.

Currently, although "[e]very State has an obligation to exercise moderation and restraint in invoking jurisdiction over cases that have a foreign element, and they should avoid undue encroachment on the jurisdiction of other States," jurisdiction remains a contentious issue. It is one of the stumbling blocks to international regulation of the Internet. Since ideology strongly influences the type of regulation used to control the Internet, there is little chance of an easy resolution.

164. See Nash, supra note 89, at D4.
165. See Knoll, supra note 93, at 288-89.
166. But see Dennis, supra note 104 (noting that German Internet regulation only extends to material uploaded from German-based computers).
167. See Hanley, supra note 129, at 1010.
168. Id.
169. See supra Part II.C.
170. Feir, supra note 105, at 384.
171. See id. at 376-82
173. Wilske & Schiller, supra note 131, at 126.
3. Enforcement of Regulations

Nations face difficulties enforcing regulations governing Internet use. The enforcement provisions must be directed at the appropriate target. Currently, Germany and China hold ISPs responsible for the content of Internet sites, while the United States and China aim liability at the individuals that post objectionable content on the web. Both regulatory regimes are flawed.

Holding ISPs responsible for Internet content raises a number of problems. First, ISPs are not technically responsible for creating the content of Internet sites. These companies merely provide their subscribers access to the Internet. The subscribers create the web sites. Also, "if the ISPs were held accountable for information content, the efforts required to censor the immense amount of material traveling across the Internet would overwhelm ISPs." Furthermore, holding ISPs liable for Internet content can have drastic results. As Germany discovered, companies often take radical action to limit responsibility when threatened with liability. This radical action at one point shut down 1500 innocent web sites and cut off four million users in 146 countries from discussion groups. ISPs simply do not have the technology to block only certain subscribers from content on the web. Current technology only allows an all-or-nothing solution. Accordingly, since each country has a different standard of tolerable speech and the ISPs cannot block content based on the country of origin, ISPs would simply apply the highest level of scrutiny to any objectionable site.

On the other hand, holding individuals liable for the content of a web site carries a different enforcement problem. As a global phenomenon, it is very difficult and costly to track down specific Internet users that post objectionable content. "Traffic analysis may not disclose the information content, however, the source and destination can suggest certain interests. Once again, the vast structure of the Internet renders this solution untenable." The United States uses individual liability to regulate Internet content,

---

174. See supra Parts II.B-C.
175. See supra Parts II.A, C.
176. See supra note 74.
177. Hanley, supra note 129, at 1008.
178. See Knoll, supra note 93, at 287-89.
179. See id.
180. See Meyer, supra note 83, at 65.
181. See id.
182. See Delacourt, supra note 61, at 213.
183. See Hanley, supra note 129, at 1008 & n.62. Hanley calls this solution "patrolling the Internet." Id.
184. "Traffic analysis" refers to tracking the movements of individuals on the Internet. However, this technology is limited to tracking the web sites visited, not the content accessed.
185. Hanley, supra note 129, at 1008-09 (footnote omitted).
e.g. prohibiting individuals from downloading child pornography. Pre-existing U.S. statutes concerning the interstate transmission of obscenity have been applied to users downloading such material from the Internet; however, finding the individuals that traffic in child pornography and obscenity is far more difficult than criminalizing such behavior.

China also attempts to control the Internet by regulating users. Article 13 of China's (Interim Internet Management) Rules lists as illegal activities: transmitting information that is "prejudicial to state security;" leaking "state secrets;" "produce, retrieve, duplicate, and disseminate information prejudicial to public order;" and "pornographic materials." However, "[d]efinitions of state security, state secrets, or public order are not provided." The broadness of this provision masks its technical ineffectiveness. Although China may outlaw certain conduct, like the United States, it must find a way to catch those responsible first.

4. Policy Concerns

Policy concerns behind Internet regulation generally coincide with the nation's ideology. "Foreseeable problems arise in enforcing international laws enacted to regulate the Internet since countries hold vastly different political and social values." When nations examine Internet regulation, they often evaluate degrees of control. For example, the constitutions of the United States and Germany guarantee protection for certain behavior, requiring inquiry into how much control of the Internet is constitutionally permitted. In the United States, the Supreme Court protects Internet users by reviewing regulations for comportment with the Constitution and striking down those which fail to pass Constitutional muster. But "[f]reedom of speech is not a universally held belief. Problems inevitably arise when a country such as Germany wishes to prosecute a United States citizen for placing pro-Nazi propaganda on the Internet." While China does not protect certain freedoms like the United States and Germany, it must also consider the degree to which it will regulate the Internet. Nevertheless, instead of using personal freedoms to limit regulation, the Chinese government regulates the entire Internet and limits personal access. The Chinese government assumes the role of determining...

189. Text of Interim Internet Management Rules, supra note 64, at art. 13.
190. Feir, supra note 105, at 371.
191. Hanley, supra note 129, at 1010.
194. Hanley, supra note 129, at 1010.
195. See supra Part II.C.
the morality of Internet content, a constitutionally untenable position for the United States and Germany.

B. Theoretical Problems with Regulating the Internet

While practical problems hinder nations' efforts, the difficulties with Internet regulation do not stop there. Nations must also determine who should regulate the Internet. The three choices are: (1) private regulation by corporations,\(^{196}\) (2) public regulation by nations,\(^{197}\) and (3) regulation by international law.\(^{198}\)

1. Private Regulation by Corporations

Enforced through ISP liability, nations can regulate the Internet by holding ISPs responsible for promulgating rules to conform subscribers' web sites. The government would not need to track offenders or update regulations for technological changes, leaving corporations responsible instead. Currently, although the United States imposes some ISP liability,\(^{199}\) Germany and China both hold corporations primarily responsible for Internet content.\(^{200}\)

As nations find it difficult to enforce their laws against individuals in other countries, nations' power over resident corporations is important.\(^{201}\) Other nations are often unwilling to extradite citizens based on alleged web offenses, since nations have different protections for free speech.\(^{202}\) Nonetheless, a resident corporation usually will prove more responsive to threats of prosecution because it has a tangible stake in the country. Since the corporation has assets invested in the country, the threat of prosecution, including confiscation of assets, can be severe, guaranteeing that the corporation will take action to forestall prosecution.\(^{203}\) Furthermore, assuming that private corporations are profit-maximizing entities, they are necessarily more responsive to technological shifts since profit margins drive their competitive ability.\(^{204}\) Nations would no longer have to worry about specific laws becoming outdated as technology changes.

Nevertheless, allowing corporations to police the Internet does have its drawbacks. Assuming again that corporations are profit-maximizing entities, their decisions may be governed by simple cost-benefit analyses, only

---

\(^{196}\) See supra Parts II.B-C (discussing German and Chinese attempts to hold ISPs liable for Internet content).

\(^{197}\) See supra Parts II.A-B (discussing U.S. and German attempts to legislate against objectionable content).

\(^{198}\) See Hanley, supra note 129, at 1009-11.

\(^{199}\) See 47 U.S.C. § 223(a)-(h) (1996). Unlike Germany and China, the United States enacted a provision allowing limited or no liability for ISPs that could demonstrate a good faith effort to screen out underage users. See § 223(c); cf. 47 U.S.C. § 230(c) (1996) (limiting liability for ISP's role as speaker or publisher of user's posted material).

\(^{200}\) See supra Parts II.B-C.

\(^{201}\) See Hanley, supra note 129, at 1010; see also supra Part III.A.2.

\(^{202}\) See id.

\(^{203}\) See Nash, supra note 89, at D4; see also Knoll, supra note 93, at 287-89.

\(^{204}\) In contrast, a government entity's motivation will be based on public interest, not survival, and thus may not be as compelling.
asking whether allowing access makes sense from a bottom-line perspective. Most nations can easily levy fines that affect the bottom-line, and corporate executives will certainly be unwilling to endure prison terms for their profit margin. Yet, as indicated by Germany's threats of prison terms for CompuServe's officials, corporate response to threats often will be overinclusive because the corporation will seek to eliminate any basis for liability. Facing potential legal liability, corporations will tend to censor Internet content strictly. In the United States, at least, this government-compelled censorship would infringe on the protections afforded by the Constitution.

Furthermore, from a policy perspective, holding corporations vicariously liable for the actions of private individuals seems inappropriate when it will not have any significant impact on those who upload objectionable content to the Internet. Individuals need only shop in a favorable jurisdiction for ISPs with deep pockets. Unfortunately, despite the inherent difficulties with regulating the Internet through private corporations, it is the most likely course of action. "[T]he architecture of a flexible system which supports both government censorship and self-regulation" is only possible through one method: "the common thread being government control over ISPs."

2. Public Regulation by Nations

While national regulation is the most popular reaction to Internet control, it is by no means the most effective. "Currently, each nation finds it difficult, if not impossible, to control Internet transmissions past its borders . . . ." In the United States, in particular, government Internet regulation has proven ineffective, and the government is struggling to reconcile Internet restrictions with the Constitution.

One problem with nations regulating the Internet is that the legislative process is too static. Internet technology changes quickly, and nations with all of their institutional inertia cannot hope to keep pace. Another concern is that nations may pass laws that attempt to regulate the Internet globally. "Internet metropolises have yet to seriously consider other nations' regulation efforts." Such broad-based regulation occurred in Germany when government pressure forced an ISP to shut down access to many innocent websites. As a result, Germany cut off access world-

205. See supra Part II.B (discussing how Germany's threat of prison terms for CompuServe's executives galvanized the company to action).
206. See Nash, supra note 89, at D4.
207. See Knoll, supra note 93, at 287-89.
208. See U.S. Const. amend. 1.
209. Hanley, supra note 129, at 1023.
210. Id. at 1022.
211. See supra Part II.A.
214. See id. at 1013-14.
215. See Knoll, supra note 93, at 287-89.
wide.\textsuperscript{216} As \textit{The Economist} protested, “When Bavaria wrinkles its nose, must the whole world catch a cold?”\textsuperscript{217}

Also, there are many practical problems intrinsic to nations regulating the Internet. Nations often cannot exercise the jurisdiction necessary to enforce their laws.\textsuperscript{218} Even when nations pass laws, they will have difficulty tracking down and/or extraditing offenders.\textsuperscript{219} Finally, on a policy level, most nations disagree as to the protection afforded certain activities.\textsuperscript{220}

However, while Germany and the United States struggle with national regulatory regimes,\textsuperscript{221} China's system has been surprisingly effective.\textsuperscript{222} China heavily censors its own Intranet and limits Internet access to a few ISPs.\textsuperscript{223} Although this system limits China's exposure to the Internet, many critics find that “Chinese authorities have shown a considerable naivete with regard to the Internet — the restrictions which they have imposed on the use of the Internet are seemingly hollow.”\textsuperscript{224} Nonetheless, China's censorship does not succeed through technological brilliance, but through intimidation.\textsuperscript{225} Western democracies will not use intimidation to enforce Internet control; thus effective regulation for them remains illusory.

3. \textit{Regulation by International Laws}

“Currently, international law governing the Internet does not exist.”\textsuperscript{226} International law has effectively regulated other modes of communication, like satellite television and telephone networks.\textsuperscript{227} Unfortunately, these forms of communication are very different from the Internet.\textsuperscript{228}

While international law does offer some hope, there are many unresolved issues. The problems with international law governing the Internet ultimately trace back to ideological differences between nations: free speech is not a universally held right, and pornography is not universally disparaged; nations simply have different standards for what they deem appropriate.\textsuperscript{229} For example, China regulates everything, limiting the

\begin{itemize}
\item \textsuperscript{216} See id.
\item \textsuperscript{217} \textit{Sex on the Internet}, \textit{The Economist}, Jan. 6, 1996, at 18.
\item \textsuperscript{218} See supra Part III.A.2 (discussing jurisdiction over offenders).
\item \textsuperscript{219} See supra Part III.A.3 (discussing the enforcement of laws).
\item \textsuperscript{220} See supra Part III.A.4 (discussing policy concerns).
\item \textsuperscript{221} See supra Parts II.A-B (examining the United States and Germany).
\item \textsuperscript{222} See supra Part II.C (examining China).
\item \textsuperscript{223} See Taylor, supra note 105, at 633.
\item \textsuperscript{224} Id. at 638.
\item \textsuperscript{226} Hanley, supra note 129, at 1009.
\item \textsuperscript{227} See, e.g., Perritt, supra note 60, at 158-60.
\item \textsuperscript{228} See supra Part III.A.1 (discussing the uniqueness of the Internet).
\item \textsuperscript{229} See Hanley, supra note 129, at 1010.
\end{itemize}
Internet to business-specific purposes;\textsuperscript{230} Germany prohibits neo-Nazi propaganda;\textsuperscript{231} and the United States targets pornography.\textsuperscript{232} These differing standards and the unwillingness to compromise make international regulation improbable. This ideological impasse would manifest itself in attempts to enforce any international law regulating the Internet.\textsuperscript{233}

Another counter-argument to international laws is that the judicial system will develop an applicable interpretation given enough time.\textsuperscript{234} Also, "[eighty percent] of the planet's population currently lacks access to basic telecommunications technology. This calls into question whether the end of the millennium is the appropriate time to harmonize legal systems for the global information infrastructure, since only [twenty percent] of the world population is participating."\textsuperscript{235} With this in mind, any international agreement would bind countries and individuals who have not even experienced the possibilities of the Internet, let alone the consequences.

IV. Non-Regulation as the Solution

Non-regulation of the Internet could be considered a controversial approach to Internet regulation. However, in light of the failed efforts to impose any coherent control over information available on the Internet,\textsuperscript{236} it is better to allow the Internet to develop and evolve before hastily intervening. When the Internet's growth has slowed and the effects of Internet use are plain, only then can the law hope to create a proper regulatory regime. For now, the governments of the world should allow the Internet to develop, grow, expand, and realize its full potential. As one commentator noted:

My point is about timing—when the balance should be drawn. There are many who now see the extraordinary expressive and associational potential that cyberspace offers. Most, however, do not. If the many prove correct, the most will eventually see the same—as the space becomes more common, as their children become transformed by it, as life takes root within it. But this seeing will take time. It will require that individuals gain an experience with this new space that gives them the sense of what this new space is. Only

\textsuperscript{230} See supra Part II.C.  
\textsuperscript{231} See supra Part II.B.  
\textsuperscript{232} See supra Part II.A.  
\textsuperscript{233} See supra Part III.A.3.  
\textsuperscript{235} Id. (footnote omitted). This observation applies a Western view to Internet development, relying on judicial review to harmonize Internet policy. This, of course, is time-consuming and reactive, as opposed to proactive.  
\textsuperscript{236} See supra Part III.
when this experience is common should we expect to be in a position to understand its significance. When the technology, when the experience, when the life in cyberspace presses us, only then should we expect law to understand enough to resolve these questions rightly.  

The Internet’s negative image has been indelibly imprinted on many minds: the Internet is wild, a hotbed of pornography and criminal activity. Accordingly, many people would believe any Internet regulation is better than none. Nevertheless, conceptualizing the Internet as a source of objectionable activity mischaracterizes most of the information available on the Internet. The last section of this Note explores and critiques the arguments made in favor of regulating the Internet and argues that some regulation is not better than none at all.

A. Concerns with Non-Regulation

There are three main concerns that drive the desire for Internet regulation: (1) the presence of objectionable content, (2) potential for criminal activity, and (3) difficulty maintaining state sovereignty. Generally, regulatory regimes target these areas. Nations intervene to ensure that what their citizens view or use will not inflict harm or disrupt government functions.

1. Objectionable Content

Pornography, hate speech, and other examples of objectionable content certainly exist on the web, and many nations seek to regulate what their citizens see. Nations enforce a certain morality where governments determine their citizens’ appropriate use of, access to, and participation in media or activities, sometimes at the behest of the citizens themselves. These citizens and their governments fear that the Internet provides easy access to objectionable content and enables its mass dissemination.

However, the fear greatly exaggerates the threat. “[M]illions of people . . . regularly use the Internet and come in contact with virtually no sexual content whatsoever.” While objectionable content exists, the

238. See Delacourt, supra note 61, at 218-20.
239. See id. at 221-23.
240. See generally Perritt, supra note 60.
241. See supra Parts II.A-B (discussing the United States targeting pornography and Germany targeting hate speech); see also Banned President Mitterand Book Posted Online, Newsweek, Jan. 25, 1996, available in 1996 WL 7906965 (describing France’s prosecution of a web site owner for displaying a book that revealed secrets about a former French president).
242. For example, lobbyists petitioned the United States government for legislation restricting access to pornographic web sites. See supra Part II.A. (exploring the CDA).
243. See supra Part III.A.1.
244. See Steven Levy, Stop Talking Dirty to Me: Let’s Hope the Media Frenzy About Sex in Cyberspace Has Almost Played its Course, Newsweek, Oct. 16, 1995, at 84.
245. Id.
Internet user decides what sites to visit and what sites to avoid.\textsuperscript{246}

In response to the concern about objectionable material available to children, many ISPs distribute software with parental controls.\textsuperscript{247} This software is arguably more effective than legislation that imposes the views of paternalistic government officials. Since it allows parents to determine the boundaries of what children should and should not see, adults would have unrestricted access to the Internet.

Parental control software may help dispel the belief that the Internet is "wild."\textsuperscript{248} Contrasted with ponderous and often blundering national legislation, parental controls provide a relatively painless way to regulate user activity.\textsuperscript{249} Therefore, since the Internet's beneficial uses far outweigh the actions of individuals intent on uploading objectionable material, stunting the growth of the Internet through ill-advised regulations would be a hasty response to an illusory problem.

2. Criminal Activity

"A further concern voiced by proponents of Internet regulation is that without some form of intervention the Internet will become a haven for criminal activity far more serious than engaging in disfavored expression."\textsuperscript{250} The key issue is whether the Internet provides technology-savvy criminals unlimited opportunities to take advantage of average citizens. But "[l]ike the hazards of objectionable on-line content, however, the hazards of on-line crime tend to be exaggerated."\textsuperscript{251}

While Internet crime does exist,\textsuperscript{252} most often it would be categorized as larceny\textsuperscript{253} or fraud.\textsuperscript{254} Better encryption technology and further education for the unwary as to the dangers of Internet communications would resolve most concerns. Moreover, it is difficult to see why an individual, already knowingly committing a crime, would view further national regulation as a deterrent.


\textsuperscript{247} See supra Part I.B.1.b. The need for parental control software was dictated by market demand, not by any law or government pressure. Furthermore, "[a] group of on-line businesses has already agreed to distribute screening software free of charge, which signifies that anyone who has the resources to access the Internet also has the resources to obtain screening software." Delacourt, supra note 61, at 231.

\textsuperscript{248} See Delacourt, \textit{supra} note 61, at 207-08.

\textsuperscript{249} See \textit{id.} at 229-34.

\textsuperscript{250} \textit{Id.} at 221.

\textsuperscript{251} \textit{Id.} at 222.

\textsuperscript{252} See \textit{id.}

\textsuperscript{253} See \textit{id.} at 221-23. Larceny involves the stealing of credit card numbers or software, both of which can be transmitted electronically and account for billions of dollars in industry losses. See \textit{id.} at 221.

\textsuperscript{254} See Branscomb, \textit{supra} note 164, at 1641-43. The Internet allows anonymity beyond that of conventional face-to-face communications. Thus, representing oneself as someone different is far easier. See \textit{id.}
3. Sovereignty Concerns

Sovereignty concerns also drive nations to regulate the Internet.\textsuperscript{255} Nations zealously guard their sovereignty and perceive the Internet as a threat.\textsuperscript{256} One reason for this distrust is the Internet's global nature.

The Internet is a revolutionary phenomenon. It is not just a technology, but a way of organizing and connecting human activity, which emphasizes decentralization, specialization, and global cooperation. It is not merely a means for facilitating existing market and political institutions, but a way of redefining them altogether . . . . Unlike traditional sovereign states which are tied to geographic boundaries, the Internet is inherently global and indifferent to geographical political boundaries . . . .

. . . International law must deal with the Internet.\textsuperscript{257}

By transcending national boundaries, the Internet raises a host of concerns for nations. Totalitarian political regimes can no longer insulate their population from information disseminated by the outside world. Unlike other technologies, Internet access is relatively easy, a computer and phone line reveal a realm of unregulated information.\textsuperscript{258} In sum, nations fear that the Internet will deprive the government of substantial political control.

However, totalitarian regimes are not the only nations concerned with Internet regulation. Both the U.S. and E.U. governments must ensure that the Internet and citizens' use comport with established legislation and national constitutions.\textsuperscript{259} Since most of these countries already have complex economic linkages that secure informational freedom, they are not concerned that the Internet will destabilize the government.\textsuperscript{260} Instead, these countries worry about the tangible issues of Internet crime and the continuing enforcement of legislation against activities that are already heavily regulated, like gambling and pornography.

B. Benefits of Non-Regulation

The biggest myth associated with non-regulation of the Internet is that the web will run out of control; criminal activity and objectionable content will flourish. As explored earlier, however, the most common complaints about the Internet cannot be solved by government regulation.\textsuperscript{261} In fact, government regulation would make little or no difference in preventing these problems.

\textsuperscript{255} See generally Perritt, supra note 60.
\textsuperscript{257} Perritt, supra note 60, at 162 (footnote omitted).
\textsuperscript{258} See Perritt, supra note 60, at 161.
\textsuperscript{260} See Perritt, supra note 60, at 162-63.
\textsuperscript{261} See supra Part III.
Furthermore, non-regulation does not mean the government must turn a blind eye to everything on the Internet. Internet abuse can be dealt with under preexisting regulations. Also, Internet transactions can be taxed, with rates differing based on the content of web sites.\(^{262}\) Non-regulation would avoid confrontations with other nations over jurisdiction, enforcement, and ideological differences, but would leave room for the Internet users to self-regulate based on perceived national standards.

C. The Internet and Self-Regulation

Demonstrated by its response to parental concerns about objectionable content, Internet users and ISPs have been regulating themselves.\(^{263}\) Governmental pressure, the mere threat of legislation, is many times the only catalyst Internet users and ISPs need to restrict or refrain from conduct. "Persons in countries which heavily regulate or monitor the Internet may also voluntarily restrict their communications to avoid criminal sanctions."\(^{264}\) More specifically, in China, "self-censorship on the Internet will occur as it does in the print media with journalists wishing to avoid governmental scrutiny."\(^{265}\) Internet users and ISPs are responsive and adaptable, acting much like any free market. Thus, external pressures can certainly influence behavior more effectively than overbearing and territorially confined regulations.

Conclusion

This Note began by comparing the Wild West of the United States in the 1800s with the electronic frontier of the Internet today. The similarities exist: little regulation and numerous new opportunities. Yet this is where the similarities end. Whereas the United States successfully tamed the West with federal regulation that controlled its development, a similar approach to taming the Internet is unworkable. Periodic government enforcements, like Germany's showdowns with CompuServe and America Online\(^{266}\) and the United States' duel with the ACLU over the CDA,\(^{267}\) are the first haymakers in the brawl. Each nation strives to stay abreast of ever-changing Internet technology; however, increasingly, governments are losing these fights. Despite the availability of several regulatory tools, no previously used methods are suited regulating the Internet.

Nations cannot enlist ISPs to regulate the Internet because no corporation can effectively control the content subscribers access. It is too simple to circumvent efforts by ISPs to restrict access to objectionable sites.\(^{268}\)

---

262. The government currently taxes cigarettes highly; similarly high rates here could amount to an "e-sin" tax that encourages web sites to restrict objectionable content.

263. See supra note 248 and accompanying text; see also Knoll, supra note 93, at 278.

264. Knoll, supra note 93, at 278.

265. Feir, supra note 105, at 384.

266. See supra Part II.B.

267. See supra Part II.A.

268. See supra Part II.B (describing the use of mirror sites to counteract T-Onlines blocking of objectionable web sites).
Thus, holding private corporations responsible for regulating Internet content leads to results like what transpired in Germany, where companies overreacted to government threats and barred access to "innocent" sites in an effort to divest liability.° Private corporations may be responsive to the continuing development of technology, but are not large enough to wield any discernable influence over Internet users.

Nor can national regulation effectively govern the Internet. The United States encountered difficulty in prescribing broad means to restrict Internet content, unenviably captive to its own Constitution. On the other end of the spectrum, China's forced censorship is at best a temporary sandbag wall before the floods of information force their way into the country. China controls its people's Internet access more through fear and intimidation than by regulation of technology.

International laws are probably the most effective way to enforce Internet regulations, but the likelihood of international consensus remains slim. Even among the three leading nations, there is little concurrence as to how much free speech to tolerate. The United States, Germany, and China cannot possibly agree on content restrictions, much less if countries like Singapore and India were involved.

The simplest, albeit most frightening, solution leaves the Internet unregulated. While seemingly shocking and morally lax, non-regulation prevents overbroad application of laws that will hinder the growth and development of the Internet. Nations can scramble to tailor laws that will govern the Internet, but the Internet's infrastructure adapts to avoid such localized laws quickly. The Internet's global nature makes it impossible to control and impossible to damage; the Internet was designed to be immune to catastrophes and invulnerable to shut down. Similarly, Internet regulation may be seen as an attack and, as such, will be circumvented. While nations try to keep pace with this ever-changing technology, the world's governments may be doomed to haplessly chasing the Internet into the sunset.

269. See supra Part II.B.
270. See supra Part II.A.
271. See Taylor, supra note 105, at 638.
272. See Hanley, supra note 129, at 1010.
273. See supra Part I.A.