NOTES

WHEN SPEECH IS HEARD AROUND THE WORLD: INTERNET CONTENT REGULATION IN THE UNITED STATES AND GERMANY

JOHN F. MCGUIRE*

> [T]he fury of the cyber-revolution is quite well advanced. The struggle over defining what cyberspace will be has the feel of the French Revolution. People are shocked at the tone of the debate, terrified at the fury. And one is well advised in such a context not to step out of line.[1]

INTRODUCTION

Frankie, a ten-year old American student, accesses the Internet[2] through his home computer to learn more about the Executive Branch for a school social studies project. To access the official home page of the President, Frankie uses the America Online web browser[3] to type the Internet address "whitehouse.com." Upon entering the address, however, Frankie is surprised as his screen reveals lewd, par-

* The author would like to thank Professors Yochai Benkler and William Nelson for thoughtful suggestions and support throughout the development of this Note. Melanie Hochberg, Troy McKenzie, Inna Reznik, the staff of the *New York University Law Review*, and especially Jennifer Lyons provided helpful comments and superb editorial assistance.

1 Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 Jurimetrics J. 629, 633 (1998) (commenting upon vociferous debate between those who advocate legislative regulation of Internet and those who advocate technological solutions).

2 The Internet is the much-heralded worldwide network of over 50,000 individual computer networks that allows computer users to communicate with computers on any other network in the system. See Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997) (describing Internet technology). The networks are composed of personal users, government agencies (such as the Executive Branch homepage in this hypothetical example), educational institutions, and corporations in 145 countries. See Carol Lea Clark, A Student's Guide to the Internet 5 (1996) (providing detailed introduction to Internet technology and evolution). For an introduction to Internet technology, see generally Raymond Greenlaw & Ellen Hepp, In-line/On-line: Getting Things Straight on the Internet (1997).

3 Computer users can access the Internet by joining a commercial or private Internet service provider (ISP) such as America Online, CompuServe, or Microsoft Network. See *Reno*, 117 S. Ct. at 2334. ISPs include browsers that organize information posted by individuals or organizations in the form of websites, and allow users to search the World Wide Web by content or keyword.

tially naked photos and obscene language. He has stumbled inadvertently onto a pornographic website.[4]

Simultaneously, Dagmar, a German graduate student, is conducting political research on the Internet. During one of her World Wide Web searches, she runs across a neo-Nazi website posted by a political extremist in Toronto.[5] Unbeknownst to Dagmar, she has stumbled inadvertently onto a website that is illegal in her country. German bureaucrats have monitored the home page and are preparing to prosecute the German Internet service provider (ISP) that provided her access to the site.[6]

• • •

The above juxtaposition highlights some of the difficulties countries face when they attempt to map domestic policy goals onto a borderless technology that, by its nature, resists unilateral control. The exponential growth of Internet use around the world[7] has prompted many governments to implement regulation of undesirable online content. This Note examines attempts by the United States and Germany to regulate Internet content within their borders and analyzes the different and sometimes conflicting legal constraints that operate in both countries. Though western democracies with similar constitutional protection of free speech,[8] the United States, with a focus on pornography, and Germany, with a focus on extremist political speech, disagree on what sorts of content should be regulated on the

[4] The correct Internet address for the White House is "whitehouse.gov." See <http://www.whitehouse.gov> (visited Feb. 20, 1999). The whitehouse.com website, see <http://www.whitehouse.com> (visited Feb. 20, 1999), is but one example of a sexually explicit website that has received significant media attention. See, e.g., Today: Interview: Donna Rice Hughes (NBC television broadcast, Sept. 17, 1998), available in 1998 WL 13521918 (discussing her book, Kids Online, and pornography problems on Internet). While the "whitehouse.com" website is marked "Over 18 Only" and requires membership for access beyond the welcome page, see <http://www.whitehouse.com> (visited February 20, 1999), this may offer little comfort to a surprised Frankie and his parents. Internet web browsers and software that have the capability to screen out such objectionable material currently are available to parents. See infra Part III (describing screening technology).

[5] This hypothetical is based on the German prosecution of Bertelsmann Online, a German ISP, for providing access to a Canadian extremist homepage in contravention of German law criminalizing the promulgation of rightist propaganda. See infra text accompanying note 108.

[6] See infra text accompanying note 108. Similar prosecutions can occur under a German Internet content control bill if adequate technological means are not employed to screen out illegal content. See infra notes 111-14 and accompanying text.

[7] An estimated 175 million people worldwide have access to the Internet. See Global Internet Statistics (visited Apr. 3, 1999) <http://www.euromktg.com/globstats>. In 1997, the *Reno* Court estimated that 40 million people had access to the Internet, a number that was expected to quintuple by 1999. See *Reno*, 177 S. Ct. at 2334.

[8] Compare infra Part I.A (describing free speech protection in Unites States), with infra Part I.B (outlining free speech protection in Germany).

Internet. These divergent interests of two similar nations display the need for a decentralized system of regulation that is flexible enough to achieve domestic regulatory goals while avoiding rigid, governmentally dictated content control. This Note argues that a market-driven regulatory system combining an Internet ratings regime with screening software may provide the best method to achieve two goals: (1) internalization of domestic legal constraints in an Internet regulatory regime; and (2) preemption of more drastic legislative regulation that may be politically expedient in the United States, Germany, or elsewhere.[9]

Part I focuses on the free speech frameworks and the incidents of Internet regulation in the United States and Germany. This Part emphasizes the political pressures that led each country to adopt legislative regulation of the Internet. Part II places the efforts of these two countries to control Internet content in the context of available regulatory regimes. Part III argues that a decentralized system of flexible ratings and a market for screening software can address the legal constraints that the United States and Germany face regarding viable content regulation. Such a system would keep as much content control as possible in the hands of Internet users, rather than governments. It also would allow individuals (like Frankie's parents) and governments (like those concerned about Dagmar's political interests) to implement their preferences or laws on the Internet in a way that is least disruptive to the speech rights of other users.

I

FREE SPEECH AND INTERNET CONTENT CONTROL IN THE UNITED STATES AND GERMANY

This Part will provide a baseline understanding of First Amendment jurisprudence in the United States and explain its application to legislative efforts to regulate the Internet. Next, German free speech protections and theory will be outlined, followed by an analysis of Germany's strict legislative approach to Internet content control. Both sections highlight political pressures and legal proscriptions that necessitate some form of Internet content control.

[9] See infra Part III for examples of current proposals.

A. Speech and Internet Content Control in the United States

1. Baseline Free Speech Protection

In both theory and practice, speech is considered the most fundamental of rights in the United States.[10] Even speech that is loathsome to the hearer is protected on the theory that ideas, once exposed, will be openly debated, and the truth will win out.[11] Consequently, legislation that regulates speech on the basis of its content must overcome a strong presumption of unconstitutionality.[12]

---

[10] See U.S. Const. amend. I (stating that "Congress shall make no law abridging . . . the freedom of speech"). The Supreme Court has held that free speech is an essential cornerstone upon which our democracy is founded. See Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 641 (1994) ("[E]ach person should decide for him or herself the ideas and beliefs deserving of expression, consideration, and adherence. Our political system and cultural life rest upon this ideal."); New York Times Co. v. Sullivan, 376 U.S. 254, 269 (1964) ("'The maintenance of the opportunity for free political discussion . . . is a fundamental principle of our constitutional system.'" (citation omitted)); NAACP v. Button, 371 U.S. 415, 433 (1963) (arguing that freedom of speech is "supremely precious in our society"). The scope of this Note does not include a thorough analysis of First Amendment jurisprudence, but rather briefly introduces free speech protection principles with a focus on hate speech and obscenity, two areas especially relevant to Internet content control. For a fuller exposition of what is often complicated First Amendment doctrine, see, e.g., Geoffrey R. Stone et al., Constitutional Law 1073-86 (3d ed. 1996) (discussing historical and theoretical justifications for free speech protection); Kent Greenawalt, Free Speech Justifications, 89 Colum. L. Rev. 119, 135-40 (1989) (discussing advance of truth under conditions of freedom as opposed to some alternative set of conditions); Martin H. Redish, The Value of Free Speech, 130 U. Pa. L. Rev. 591, 601-04 (1982) (arguing that free speech serves value of individual self-realization as well as political participation); Cass R. Sunstein, Free Speech Now, 59 U. Chi. L. Rev. 255, 301-06 (1992) (arguing that First Amendment is necessary for effective political deliberation).

[11] See Brandenburg v. Ohio, 395 U.S. 444, 449 (1969) (per curiam) (striking down conviction of Ku Klux Klan leader because statute forbade "mere advocacy and . . . assembly with others"); United States v. Schwimmer, 279 U.S. 644, 654-55 (1929) (Holmes, J., dissenting) (arguing that Constitution makes imperative "the principle of free thought—not free thought for those who agree with us, but freedom for the thought that we hate"). The centrality of speech to our system of government is predicated in part on the theory that a "marketplace of ideas" is essential to a well-functioning democracy. See Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (arguing that "the best test of truth is the power of the thought to get itself accepted in the competition of the market," a process that is essential to democratic government and that requires broad freedom of expression); see also Whitney v. California, 274 U.S. 357, 375-76 (1927) (Brandeis & Holmes, JJ., concurring) (concluding that Founders believed "that public discussion is a political duty; and that this should be a fundamental principle of the American government"); Stanley Ingber, The Marketplace of Ideas: A Legitimizing Myth, 1984 Duke L.J. 1, 2-4 (noting that "[i]n addition to its usefulness in the search for truth and knowledge, the marketplace came to be perceived by the courts and scholars as essential to effective popular participation in government").

[12] See, e.g., R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) ("The First Amendment generally prevents government from proscribing speech . . . because of disapproval of the ideas expressed."); FCC v. Pacifica Found., 438 U.S. 726, 745-46 (1978) ("[I]t is a central tenet of the First Amendment that the government must remain neutral in the marketplace

Beyond this baseline of stringent protection of free speech, it is clear that the Supreme Court has limited the breadth of protection offered to some types of speech.[13] Two categories of speech, hate speech and obscenity, provide useful examples of the Court's attempt to weigh the right to free speech against countervailing values; these categories are especially relevant to a discussion of speech rights on the Internet.[14] Despite the inflammatory nature of hate speech,[15] the Court has declared restrictions on hate speech unconstitutional. In one paradigm case, *R.A.V. v. St. Paul*,[16] the Court struck down a city's ordinance that made it a misdemeanor to burn a cross, a swastika, or another inflammatory symbol to arouse "'anger, alarm, or resentment in others on the basis of race, color, creed, religion or gender.'"[17]

---

of ideas."); Police Dep't v. Mosley, 408 U.S. 92, 95 (1972) (explaining that content-based regulations are presumptively invalid).

[13] See, e.g., Konigsberg v. State Bar, 366 U.S. 36, 49 (1961) ("[W]e reject the view that freedom of speech and association . . . as protected by the First and Fourteenth Amendments, are 'absolutes.'"); Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942) (stating that it "is well understood that the right of free speech is not absolute").

Specifically, the Court has held that First Amendment protection does not extend to obscenity, see Roth v. United States, 354 U.S. 476, 485 (1957) (holding that obscene speech is not protected by First Amendment), child pornography, see New York v. Ferber, 458 U.S. 747, 773 (1982) (upholding statute prohibiting promotion of sexual performances by child under age of 16 through distribution of child pornography), libelous speech, see *Sullivan*, 376 U.S. at 279-80 (holding that libelous statements made with "actual malice" are not protected by First Amendment), "fighting words," *Chaplinsky*, 315 U.S. at 572 (1942) (defining "fighting words" as words "which by their very utterance inflict injury or tend to incite an immediate breach of the peace"), or words calculated to incite lawless action, see Schenck v. United States, 249 U.S. 47, 52 (1919) (ruling that free speech protection does not extend to words that create a "clear and present danger" of narrowly defined substantive evil).

[14] See infra Part I.A.2 (discussing application of restrictions on hate speech and obscenity to Internet).

[15] For a fuller exposition of hate speech doctrine, see, e.g., Mark A. Graber, Old Wine in New Bottles: The Constitutional Status of Unconstitutional Speech, 48 Vand. L. Rev. 349 (1995) (noting that every generation insists that First Amendment does not apply to some category of speech, such as hate speech, but arguing that value of free speech remains constant and should be maintained); Mari J. Matsuda, Public Response to Racist Speech: Considering the Victim's Story, 87 Mich. L. Rev. 2320, 2357 (1989) (arguing that hate speech directed against minority groups is so dangerous that "it is properly treated as outside the realm of protected discourse"); Terry A. Maroney, Note, The Struggle Against Hate Crime: Movement at a Crossroads, 73 N.Y.U. L. Rev. 564, 569 (1998) (recommending anti-hate crime movement recommit to "challenging the very institutions of criminal justice with which it now cooperates").

[16] 505 U.S. 377 (1992).

[17] Id. at 380 (quoting St. Paul, Minn., Legis. Code § 292.02 (1990)). The Court reasoned that the ordinance violated the principle of "content neutrality" in targeting speech that espoused supposedly unacceptable viewpoints. See id. at 391-92. See generally Laurence H. Tribe, American Constitutional Law § 12-3, at 794-804 (2d ed. 1988) (explaining requirement of content neutrality in speech restrictions). Efforts to combat hate speech extend to universities and other nongovernmental forums, often without success. See Doe v. University of Michigan, 721 F. Supp. 852 (E.D. Mich. 1989) (invalidating uni-

While sympathetic to the concerns of minorities and the incidence of hate crime,[18] the Court found that the centrality of free speech to our system of democracy trumped restrictions on hate speech that is offensive to some or all of its hearers.[19]

On the other end of the speech protection spectrum stands obscenity, an arena in which government interests in regulation have tended to outweigh the primacy of free speech.[20] The Court has found that obscenity is not protected by the First Amendment and that the governmental interest in shielding communities from sexually explicit materials is legitimate and can outweigh free speech protection.[21] However, the precise definition of obscenity has been elusive.[22]

---

versity regulation that prohibited any person from stigmatizing individuals on basis of race, religion, gender, or sexual orientation); Charles Fried, The New First Amendment Jurisprudence: A Threat to Liberty, 59 U. Chi. L. Rev. 225, 244-55 (1992) (examining university hate speech regulations).

[18] See *R.A.V.*, 505 U.S. at 395 (stating Court's sympathy with victims of hate speech).

[19] See id. at 393-94. The strong speech protection afforded hate speech in the United States contrasts sharply with the severe restrictions on such expression in Germany. See infra Part I.B.1.

[20] For a more detailed discussion of what is often complicated obscenity doctrine, see Tribe, supra note 17, § 12-16, at 904-19 (detailing history of obscenity doctrine); Shayana Kadidal, Obscenity in the Age of Mechanical Reproduction, 44 Am. J. Comp. L. 353, 379-83 (1996) (outlining theoretical and practical differences between approaches to obscenity in Germany and United States); P. Heath Brockwell, Comment, Grappling with Miller v. California: The Search for an Alternative Approach to Regulating Obscenity, 24 Cumb. L. Rev. 131, 138-45 (1994) (arguing for conduct-based approach to obscenity definition). For the Supreme Court's analysis of the history of obscenity doctrine, see generally Erznoznik v. City of Jackonsville, 422 U.S. 205, 208-17 (1975) (outlining background history of obscenity prosecutions); Miller v. California, 413 U.S. 15, 18-30 (1973) (same).

This strict treatment of obscenity may be due in large part to the more conservative manner in which American society has treated sex and sexual expression throughout the nation's history; such "puritanism" in the United States stands in contrast to many European countries' views of the subject. See Kadidal, supra, at 356-70 (outlining theoretical and social attitudes toward sexual expression). In Germany, for example, free speech restrictions, such as banned political or hate speech, tend to be upheld, while obscenity, though often a target of governmental regulation, is not as central a policy concern. See infra Part I.B.1. Interestingly, scholars have noted that the Court's concern with obscenity evidenced in Miller was a shift from previous years when it seemed the Court was "poised to do away with obscenity laws." Marjorie Heins, Sex, Sin and Blasphemy: A Guide to America's Censorship Wars 23 (1993); Elaine M. Spiliopoulos, Legislative Update, The Communications Decency Act of 1996, 7 DePaul-LCA J. Art & Ent. L. 336, 338-44 (1997) (discussing Court's struggle with obscenity and indecency).

[21] See Roth v. United States, 354 U.S. 476, 484-85 (1957) ("[I]mplicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance. . . . [W]e hold that obscenity is not within the area of constitutionally protected speech or press."); see also Blake T. Bilstad, Obscenity and Indecency in a Digital Age: The Legal and Political Implications of Cybersmut, Virtual Pornography, and the Communications Decency Act of 1996, 13 Santa Clara Computer & High Tech. L.J. 321, 366-71 (1997) (outlining development and application of *Roth* test).

[22] Indeed, Justice Douglas lamented that the Court "has worked hard to define obscenity and concededly has failed." Miller v. California, 413 U.S. 15, 37 (1973) (Douglas, J.,

Miller v. California[23] established the Court's three-part test for determining whether material is obscene and not deserving of First Amendment protection: first, "whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest";[24] second, "whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law";[25] and third, "whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."[26]

Within these parameters, the evolution of obscenity doctrine since *Miller* has yielded further guidelines to the application of the obscenity standard. Generally, printed works meet the artistic-value prong of the *Miller* test and receive the highest level of First Amend-

---

dissenting); see also Bilstad, supra note 21, at 369 (indicating subjective nature of obscenity definition). Obscenity doctrine is further complicated by a number of exceptions that arise out of concerns for undue restrictions on speech. For example, the Court created an exception for works with serious "literary, scientific, or artistic value," in reaction to concern over increasingly strident enforcement of obscenity laws. See Jacobellis v. Ohio, 378 U.S. 184, 191 (1964). Despite such exceptions and continuing uncertainty in the definition of obscenity, recent cases have held that obscenity has no constitutional protection and may be banned outright in certain types of media. See, e.g., Alliance for Community Media v. FCC, 56 F.3d 105, 112 (D.C. Cir. 1995) (upholding restrictions on obscenity in broadcast media).

23 413 U.S. 15 (1973).

24 Id. at 24 (citations omitted). The Court went on to determine that "contemporary community standards" are not national standards, and that "[i]t is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City." Id. at 32 (citations omitted). See also Hon. Joseph T. Clark, The "Community Standard" in the Trial of Obscenity Cases—A Mandate for Empirical Evidence in Search for the Truth, 20 Ohio N.U. L. Rev. 13, 30-31 (1993) (describing nature of testimony necessary to determine appropriate community standards). Given the international and cross-border availability of Internet content, the application of local community standards can be difficult. See, e.g., infra notes 49-50 (detailing pornography prosecution of California couple under Tennessee community standards).

25 *Miller*, 413 U.S. at 24.

26 Id. While the *Miller* test can be construed quite broadly, outright bans on pornography generally are not permissible, see American Bookseller's Ass'n v. Hudnut, 771 F.2d 323, 324-25 (7th Cir. 1985) (holding that *Miller* requires offensiveness to be assessed by community standards, but that "[t]he state may not *ordain* preferred viewpoints" (emphasis added)), and mere possession of obscene pornographic materials cannot be per se illegal, see Stanley v. Georgia, 394 U.S. 557, 565 (1969) (promulgating distinction between possession and dissemination of obscene materials, and concluding that "[i]f the First Amendment means anything, it means that a state has no business telling a man, sitting alone in his house, what books he may read or what films he may watch"). Per se bans are permissible when the government interest is highly compelling, as in laws against child pornography. See Osborne v. Ohio, 495 U.S. 103, 108-09 (1990) (upholding ban on child pornography because of compelling state interest in protecting children).

ment protection,[27] while the level of free speech protection afforded to other media such as radio,[28] telephone,[29] and cable broadcasting[30] varies. Important in the Internet context, sexually explicit photographs receive less protection because they often lack a context for the trier of fact to determine whether they have redeeming value, as defined in *Miller*.[31]

A final wrinkle in obscenity doctrine is the Court's creation of a category of "indecent" materials designed to protect children from sexually explicit materials not strictly classifiable as obscene under the *Miller* test.[32] In *FCC v. Pacifica*,[33] the Court ruled that an afternoon radio broadcast of George Carlin's "Seven Dirty Words" comedy routine was unprotected indecent speech because of the common prevalence of radio broadcasts and the ready access children have to afternoon broadcasts.[34] However, in *Sable Communications v. FCC*,[35] the Court reiterated that "indecent" materials, which are potentially offensive but not "obscene," receive protection under the First Amendment, and that a facial ban on such materials is unconstitutional.[36] In *Sable*, the Court found that a ban on indecent commercial communication was overbroad and held that government regulation

---

[27] See Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974) (concluding that print communications like newspapers should be afforded highest level of First Amendment protection); see also Smith v. California, 361 U.S. 147, 152-54 (1959) (finding that booksellers are not required to check content of books to determine whether they are obscene).

[28] See Red Lion Broad. Co. v. FCC, 395 U.S. 367, 386-92 (1969) (granting qualified level of First Amendment protection to broadcast communications).

[29] See Sable Communications v. FCC, 492 U.S. 115, 117 (1989) (granting telephone communications high level of constitutional protection and holding that First Amendment protects indecent, though not obscene, speech in commercial telephone messages).

[30] See Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 636-38 (1994) (granting high level of First Amendment protection to cable communications and distinguishing more relaxed standard applied to more easily accessible media).

[31] A free-standing, sexually explicit picture like those posted on some pornographic websites tends not to be seen as part of an artistic endeavor, but rather an isolated shot focusing on the sexual act itself. See Bilstad, supra note 21, at 370.

[32] For a fuller exposition of indecency doctrine, see, e.g., Tribe, supra note 17, § 12-16, at 904-19. The protection of children has been invoked frequently in the United States to justify restrictions on free speech representing one category of hearers regarding which a legitimate governmental interest in speech restrictions has been found. See id. § 12-16, at 909 n.44.

[33] 438 U.S. 726 (1978).

[34] See id. at 748-50.

[35] 492 U.S. 115 (1989).

[36] See id. at 131 (holding that, despite government's legitimate interest in protecting children, statute banning obscene and indecent dial-a-porn was overbroad and thus unconstitutional). In order to regulate indecent speech under *Sable*, the government must indicate a compelling interest (such as protecting children) and, importantly, choose "the least restrictive means to further the articulated interest." Id. at 126.

"may not 'reduce the adult population . . . to [see] only what is fit for children.'"[37] Thus, any restriction on indecent speech must be narrowly tailored to achieve the government interest without chilling protected speech of other groups.[38] This construction has acted to limit the ability of legislators to censor the Internet in the United States.

2. *Pressure for Regulation of Internet Content*

Concern about "cyberporn," a term used to describe sexually explicit words and images of adults and children on the Internet, drives attempts to regulate online content in the United States.[39] As early as June 1995 eighty-five percent of Americans surveyed were "concerned about children seeing pornography on the Internet."[40] This widespread concern gave rise to an American online indecency debate between those who believe material inappropriate to minors should be banned from the Internet and those who argue that purging the Internet of all material unsuitable for children would infringe on adult users' First Amendment rights.[41] Opponents of Internet content regulation point to successful prosecutions under existing obscenity and

---

[37] Id. at 128 (quoting Butler v. Michigan, 352 U.S. 380, 383 (1957)).

[38] See FCC v. Pacifica Found., 438 U.S. 726, 750-51 (1978) (stating that nature of communication can depend on its context, and analogizing that "'a nuisance may be merely a right thing in the wrong place,—like a pig in the parlor instead of the barnyard'" (quoting Euclid v. Ambler Realty Co., 272 U.S. 365, 388 (1926)).

[39] As more American households, libraries, and schools accessed the Internet, see Shea ex rel. American Reporter v. Reno, 930 F. Supp. 916, 926 (S.D.N.Y. 1996) (detailing growth and scope of Internet use in United States); Greenlaw & Hepp, supra note 2, § 4.3.5, at 132 (same), public concern over and media coverage of pornography on the Internet grew. A study by a Carnegie Mellon student that surveyed Internet sites for pornography fueled public concern that the Internet was rife with obscene and indecent materials. See Marty Rimm, Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2,000 Cities in Forty Countries, Provinces, and Territories, 83 Geo. L.J. 1849, 1913-15 (1995) (reporting results of Internet research on sexually explicit sites). The report led to a Time magazine cover story that piqued concern over the medium's effect on children. See Philip Elmer-Dewitt, On a Screen Near You: It's Popular, Pervasive, and Surprisingly Perverse, According to the First Survey of Online Erotica, Time, July 3, 1995, at 38 (reporting horrors of cyberporn on Internet).

[40] Nightline (ABC television broadcast, June 27, 1995), available in Lexis, Allnews Library, Script File (quoting Princeton Survey Research Associates poll).

[41] Opponents of congressional regulation of indecent material on the Internet come from all areas of the political spectrum. A lawyer at the Electronic Frontier Foundation, a proponent of civil liberties on the Internet, stated that regulation of indecent material "would transform the vast library of the Internet into a children's reading room, where only subjects suitable for kids could be discussed." Elmer-Dewitt, supra note 39, at 42. Additionally, some commentators have discussed a constitutional amendment to protect expression regardless of the medium through which it is transmitted. See, e.g., Edward J. Naughton, Note, Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech, and State Action, 81 Geo. L.J. 409, 411 (1992) (noting amendment proposed by Laurence Tribe).

child pornography laws as proof that, despite political pressures, further censorship is not required.[42] In one successful prosecution under a general obscenity law, *United States v. Thomas*,[43] a district court held a bulletin board system (BBS)[44] operator liable for system material that violated the community standards of Tennessee. *Thomas* was the first federal criminal conviction for transmitting materials over a computer network[45] and was followed by other state cases that successfully applied existing law to the Internet context.[46]

The *Thomas* conviction caused great controversy and indicated to some the inadequacy of applying current laws to the Internet. First, proponents of stricter regulation argued that state or federal obscenity prosecutions would be rare and would not capture independently

---

Perhaps more surprisingly, Net-savvy former House Speaker Newt Gingrich (R-Ga.) expressed opposition to congressional regulation of indecent material, stating that "[i]t is clearly a violation of free speech and . . . a violation of the rights of adults to communicate with each other." Kara Swisher & Elizabeth Corcoran, Gingrich Condemns On-Line Decency Act: Opposition to Senate Version May Doom Bill, Wash. Post, June 22, 1995, at D8; see also Dawn L. Johnson, Comment, It's 1996: Do You Know Where Your Cyberkids Are? Captive Audiences and Content Regulation on the Internet, 15 J. Marshall J. Computer & Info. L. 51, 59 (1996) (outlining broad disapproval of governmental censorship on Internet).

42 See, e.g., Johnson, supra note 41, at 79-85. For federal obscenity law, see generally 18 U.S.C. §§ 1461, 1462 (1994) (outlawing mailing obscene matter or transporting it in interstate or foreign commerce); id. § 1464 (outlawing broadcasting obscene language). Forty-five of the 50 states have some type of obscenity statute. See Robert A. Jacobs, Comment, Dirty Words, Dirty Thoughts and Censorship: Obscenity Law and Non-Pictorial Works, 21 Sw. U. L. Rev. 155, 171 nn.110-12 (1992) (listing state obscenity laws); J. Todd Metcalf, Note, Obscenity Prosecutions in Cyberspace: The Miller Test Cannot 'Go Where No [Porn] Has Gone Before,' 74 Wash. U. L.Q. 481, 489 n.51 (1996) (same). Responding to parental pressures, some states have enacted statutes specifically targeted at obscene material on the Internet. See, e.g., Ga. Code Ann. § 16-12-100.1 (1996) (criminalizing electronic furnishing of obscene material to minors). Moreover, most states have legislation against child pornography. See, e.g., 720 Ill. Comp. Stat. Ann. 5/11-20.1 (West 1994 & Supp. 1998); see also id. note (Comparative Laws) (listing comparative child pornography laws of 47 other states); New York v. Ferber, 458 U.S. 747, 762 (1982) (holding that state may regulate child pornography within bounds of First Amendment if statute is narrowly tailored to achieve compelling interest of protecting minors).

43 74 F.3d 701 (6th Cir. 1996). The Thomases were charged under a federal obscenity law prohibiting the knowing transport in "interstate or foreign commerce" of any obscene materials, as defined by the community standards of the prosecuting jurisdiction. See id. at 706.

44 BBS technology is similar to UseNet newsgroups, in which persons with similar interests can access and relay information on an area of specific interest. See Robert F. Goldman, Note, Put Another Log on the Fire, There's a Chill on the Internet: The Effect of Applying Current Anti-Obscenity Laws to Online Communications, 29 Ga. L. Rev. 1075, 1086-88 (1995) (describing various contemporaneous Internet technologies).

45 See Aaron Zitner, A Byte in the Law: Copyright, Libel and Obscenity Statutes Stretch to Keep up on the Electronic Frontier, Boston Globe, Jan. 15, 1995, at 33.

46 See, e.g., People v. Poplaski, 616 N.Y.S.2d 434, 436 (N.Y. Crim. Ct. 1994) (prosecuting Internet user for engaging young boys in sexually explicit conversation).

posted obscene or indecent material.[47] Second, proponents of specific Internet regulation argued that obscenity and other laws were written to address printed materials and more easily controlled media and did not adequately address the Internet.[48] Third, the case presented jurisdictional difficulties that were sure to complicate future prosecutions.[49] The Thomases posted their information in California but were prosecuted according to Tennessee's "community standards," as applied by a Tennessee jury.[50]

Because of the political pressure regarding the concern for children and the perceived inadequacy of existing laws, Congress responded with the Communications Decency Act of 1996 (CDA).[51] The CDA, which prohibited the use of an interactive computer service to knowingly transmit, send, or display any "indecent" or "obscene" material to minors, became law on February 8, 1996.[52] While the

---

47 For example, BBS operators are private content providers who require active subscribers to pay a fee to access data available on their bulletin board. See Clark, supra note 2, at 5 (providing detailed introduction to BBS and other Internet technology). They therefore are more easily identifiable than individual website content providers, making BBS and UseNet operators easier targets for liability. See Bilstad, supra note 21, at 324-25. Thus, such prosecutions would fail to capture individual content providers who account for the vast majority of Internet content. See Shea ex rel. American Reporter v. Reno, 930 F. Supp. 916, 926 (S.D.N.Y. 1996) (outlining number of content providers on Internet).

48 See, e.g., It's In the Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 14 (Wis. Ct. App. 1995) (noting that state's defamation statute was enacted "years before cyberspace was envisioned"); see also Howard L. Steele, Jr., Comment, The Web that Binds Us All: The Future Legal Environment of the Internet, 19 Hous. J. Int'l L. 495, 497 (1997) (indicating inadequacy of current laws).

49 Jurisdictional difficulties of prosecuting service providers, content providers, or users have been well documented and will be addressed only in passing here. For a fuller exposition of jurisdictional problems in Internet administration and regulation, see generally Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 Ind. J. Global Legal Stud. 475 (1998); Henry H. Perritt, Jr., Jurisdiction in Cyberspace, 41 Vill. L. Rev. 1 (1996).

50 See United States v. Thomas, 74 F.3d 701, 705 (6th Cir. 1996). It is possible that the application of the "community standards" of California would have led to an acquittal under *Miller*. See supra note 24 (noting divergence of community standards within United States).

51 Pub. L. No. 104-104, 110 Stat. 133 (1996) (codified in scattered sections of 47 U.S.C.). It is clear that the Communications Decency Act of 1996 (CDA) arose out of political pressures from concerned parents influenced by the publicity surrounding cyberporn. Indeed, the original sponsor of the CDA, Senator James Exon (D-Neb.), proposed the Act "to make this exciting new [information] highway as safe as possible for kids and families to travel." Sen. J. James Exon, Should the Plug be Pulled on Cyberporn? Keep Internet Safe for Families, Dallas Morning News, Apr. 9, 1995, at J1. The Supreme Court eventually deemed relevant parts of the CDA unconstitutional. See infra notes 63-65 and accompanying text.

52 In pertinent part, Section 502 of the Communications Decency Act subjected to criminal penalties any person who:

(1) in interstate or foreign communications—

(B) by means of a telecommunications device knowingly—

CDA's prohibitions were both elusive and sweeping, it allowed ISPs to insulate themselves from liability and invoke affirmative defenses.[53]

Additionally, there are four main points to note about the CDA. First, once downloaded material is in tangible form (on a disk or in a printout), the CDA would have been superfluous as it would have been trumped by existing laws regulating speech.[54] Second, the Act held online service providers liable for transmitting "indecent" materials only if access by minors to the website was not restricted.[55] Third, the CDA applied local obscenity and indecency standards to "interstate and foreign communications,"[56] thus raising jurisdictional difficulties on both a national and an international scale.[57] Finally, because the legal definitions of obscenity and indecency are so vague, valuable information about safe sex, reproductive health, or sex edu-

---

(i) makes, creates, or solicits, and

(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

. . . .

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity . . . .

47 U.S.C. § 223(a)(1)-(2) (Supp. II 1996). Section 223(d) was similar but focused on "patently offensive" materials. See id. § 223(d)(1)-(2). Violations of the CDA were punishable by fines up to $250,000 and jail terms up to two years. See id. § 223(a), (d).

53 The CDA provided three main defenses for ISPs. ISPs could claim a "good Samaritan" defense if they did not create or assist in the creation of prohibited content, but merely provided "access or connection to or from a facility, system, or network not under that person's control." Id. § 223(e)(1). Further, ISPs could invoke a "good faith" defense if they made "reasonable, effective, and appropriate" efforts using "any method which is feasible under available technology" to prevent minors from accessing prohibited material. Id. § 223(e)(5)(A). For example, a provider could limit its liability by identifying indecent or patently offensive material with a tag (for instance, "XXX" or "Over 18") attached to the Uniform Resource Locator (URL) or to the content page. See Spiliopoulos, supra note 20, at 350. ISPs could also satisfy this "technological alternative" defense by a system of ratings and screening software, as argued in Part III. Lastly, ISPs could be insulated from liability if they restricted access of minors by requiring the use of a "verified credit card, debit account, adult access code, or adult personal identification number." 47 U.S.C. § 223(e)(5)(B) (Supp. II 1996). Personal identification methods are employed by a number of commercial ISPs, some of whom charge for the service. See Spiliopoulos, supra note 20, at 350.

54 See Amy Knoll, Comment, Any Which Way but Loose: Nations Regulate the Internet, 4 Tul. J. Int'l & Comp. L. 275, 281-82 (1996) (arguing that CDA was not only unacceptable overregulation but also superfluous).

55 See 47 U.S.C. § 223(e)(5) (Supp. II 1996).

56 Id. § 223(d)(1).

57 See supra notes 49-50 and accompanying text (discussing jurisdictional difficulties of law enforcement on Internet).

cation could have been cut off from users.[58] This chilling effect on speech could have also affected other information on the Internet, such as art, since the penalties for violating the CDA might have caused people to restrict access to information on artists from Mapplethorpe to Michelangelo.[59]

Public response to the CDA was largely negative.[60] Importantly, the Department of Justice (DOJ) opposed the CDA because it said that it "has all the laws it needs to police the Net."[61] Legal attempts to invalidate the CDA began immediately, with opponents arguing that the provision regarding "indecent" materials was overbroad and therefore unconstitutional.[62] The challenge reached the Supreme Court, which relied on the *Sable* application of the indecency standard[63] to invalidate the CDA as it related to indecent materials.[64] The availability of technological alternatives that could tailor content regulation to protect minors without imposing a unilateral ban on content for all users was critical to the Court's decision that the CDA was not the least restrictive means to achieve the government's goals.[65]

---

58 See Ramon G. McLeod & Reynolds Holding, Telecom Bill Called Threat to Free Speech on the Net, S.F. Chron., Feb. 7, 1996, at A1 (outlining opposition to CDA and detailing effects of its provisions).

59 See id.

60 See Bilstad, supra note 21, at 379 (outlining public response). One New York Times editorial stated simply, "Cyberspace, with 20 million users worldwide, connecting 145 nations, is too rich and complex an environment for a law as general and misinformed as the Communications Decency Act." David S. Bennahum, Getting Cyber Smart, N.Y. Times, May 22, 1995, at A15. Professor Lessig derided the bill as "failed and stupid." Lessig, supra note 1, at 630.

61 Julian Dibbell, Muzzling the Internet, Time, Dec. 18, 1995, at 75.

62 See, e.g., Shea v. Reno, 930 F. Supp. 916, 923 (S.D.N.Y. 1996) (holding that overbroad CDA would ban constitutionally protected indecent communication between adults), aff'd, 117 S. Ct. 2501 (1997); ACLU v. Reno, 929 F. Supp. 824, 849 (E.D. Pa. 1996) (granting preliminary injunction to enjoin enforcement of CDA provisions that plaintiffs argued were unconstitutional), aff'd 117 S. Ct. 2329 (1997).

63 See Reno v. ACLU, 117 S. Ct. 2329, 2343 (1997) (citing Sable Communications v. FCC, 492 U.S. 115, 127-28 (1989)).

64 See *Reno*, 117 S. Ct. at 2343-50. Specifically, the Court explained that "the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech." Id. at 2346. The Court struck down 47 U.S.C. § 223(a)(1)(B), (a)(2), and (d), which made it a crime to send or display "indecency" to a minor. See id. at 2350. The Court did not declare unconstitutional other parts of the CDA, including the defenses and the portions of the Act relating to obscene material. See id. at 2350-51. The plaintiffs in *Reno* did not challenge the application of existing obscenity laws, and these laws remain applicable to the Internet.

65 See id. at 2348. The specific technological innovations to which the Court referred were ratings systems and screening software. See id.; see also infra Part III (proposing such technological solutions). But see *Reno*, 117 S. Ct. at 2349 (acknowledging in its discussion of CDA defenses that "effective" screening software did not exist at time of decision).

The defeat of the CDA, however, did not quell congressional support for government censorship of cyberspace.[66] In October 1998, congressional Republicans squeezed the Child Online Protection Act (COPA)[67] into an omnibus spending bill in the final days of the session. COPA targets those commercial websites that disseminate information "harmful to minors" without restricting underage access to such materials.[68] Substituting "harmful to minors" for "indecent" was a clear congressional effort to avoid triggering the *Sable* constitutionality test[69] that doomed the CDA.[70] Commentators and the DOJ, however, quickly claimed that COPA too would fail constitutional muster,[71] and a Pennsylvania federal judge granted a preliminary in-

---

66 In addition to the Child Online Protection Act, see infra note 67 and accompanying text, Congress introduced several bills to limit access to "harmful" materials on the Internet, including the Online Parental Control Act of 1996, H.R. 3089, 104th Cong. (1996), the Internet Freedom and Child Protection Act of 1997, H.R. 774, 105th Cong. (1997), and the Family-Friendly Internet Access Act of 1997, H.R. 1180, 105th Cong. (1997).

67 Pub. L. No. 105-277, tit. XIV, 1999 U.S.C.C.A.N. (112 Stat.) 841 (1998) (to be codified at 47 U.S.C. §§ 223, 230, 231). The Act is also somewhat derisively known as the Communications Decency Act II. For an overview of COPA's passage and the political pressures that shaped the final bill, see Neil Munro, The Web's Pornucopia, Nat'l J., Jan. 9, 1999, at 38.

68 See Child Online Protection Act of 1998, § 1403, 112 Stat. at 842. In its entirety, this section provides that:

> Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

Id. The Act provides similar "safe harbor" defenses for ISPs, see id. at 842-43, as those provided by the CDA, see supra note 53.

69 See supra notes 32-38 and accompanying text (discussing *Sable*).

70 See supra notes 63-65 (discussing invalidity of CDA due to overbreadth of "indecency" language). Congress was explicitly relying on the "harmful to minors" standard that was upheld by the Court in Ginsberg v. New York, 390 U.S. 629, 633 (1968) (upholding New York statute that prohibited sale of obscene bookstore materials considered harmful to minors).

71 In addition, the Department of Justice (DOJ) argued that COPA would divert funds from more important tasks, and that it contained several ambiguities. See Munro, supra note 67, at 43; see also David E. Rovella, New Internet Porn Law Under Attack, Nat'l L.J., Nov. 16, 1998, at A7 (detailing DOJ opposition). Indicating the immense importance of political pressure related to Internet content control, however, the DOJ publicly switched its position and supported the bill after it was clear that the Republicans in Congress were preparing to exploit DOJ and White House opposition. See Munro, supra note 67, at 42-43. According to one of the bill's supporters, "The last thing Al Gore needed was stories about how he was trying to kill a bill intended to protect kids against online porn." Id. at 40 (quoting Representative Michael G. Oxley (R-Ohio)).

Further, Internet industry associations and a number of communications companies opposed the measure, fearing that restrictive measures could hamper the Internet's money-making potential. As with Executive Branch opposition, however, some of the corporations made a public about-face and supported COPA "fearing political damage should

junction halting COPA's application.[72] While the ultimate fate of COPA is uncertain,[73] its lesson is clear: Political pressures on the United States Congress to protect children by controlling content on the Internet are strong. As argued in Part III, an alternative form of decentralized regulation is necessary to protect speech, placate voters, and preempt such efforts at government censorship in the United States. However, any viable alternative must serve not only the needs of the United States but also the larger international Internet community by allowing all countries to internalize their different legal standards.

B. Constitutional Framework and Internet Regulation in Germany

Germany provides an excellent contrast to the United States with regard to its protection of free speech and regulation of the Internet. This section outlines Germany's framework of free speech protection, which allows for far more regulation of political speech than in the United States, and then surveys Germany's vigorous legislative content control of the Internet.

1. German Free Speech Protection

The German constitutional system is grounded in the Grundgesetz, or Basic Law, which became effective in the Federal Republic of Germany in 1949.[74] While the centrality of free speech to the consti-

---

[they] be seen as opposing the bill." Id. (discussing public statements by Disney and Microsoft, two companies who initially lobbied against COPA).

[72] See American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473, 498 (E.D. Pa. 1999) (granting preliminary injunction against enforcement of COPA); see also Pamela Mendels, Setback for a Law Shielding Minors from Smut Websites, N.Y. Times, Feb. 2, 1999, at A12. For details of the litigation surrounding COPA, see John Schwartz, Online Decency Fight Brews Anew After Ruling, Wash. Post, Dec. 14, 1998, at F21.

[73] See Mendels, supra note 72, at A12 (noting that DOJ was reviewing litigation options after ruling, including appeal).

[74] The Grundgesetz was a conscious reaction to the Third Reich and the failed Weimar Republic and grew out of the unique historical circumstances of the country. See Günter Dürig, An Introduction to the Basic Law of the Federal Republic of Germany, in The Constitution of the Federal Republic of Germany 12, 12 (Ulrich Karpen ed., 1988) (describing historical background of German Basic Law); Edward J. Eberle, Public Discourse in Contemporary Germany, 47 Case W. Res. L. Rev. 797, 799-801 (1997) (discussing differences between German Basic Law, which intends to codify objective order of rights and duties, and American Constitution, which sets forth value-neutral scheme of negative liberties and rights upon which government cannot infringe).

The Basic Law was not intended to be a permanent document, but rather a transitional instrument pending national unification, when a "constitution" (*Verfassung*) would be adopted in perpetuity. See David P. Kommers, German Constitutionalism: A Prolegomenon, 40 Emory L.J. 837, 837 (1991) (detailing evolution of Basic Law). However, the Basic Law survived the test of time essentially unchanged and helped support a strong democratic state in West Germany. When the Unification Treaty was signed with East

tutional order and structure of society are similar in the United States and Germany,[75] the German experience has led to a different philosophical justification for free speech. According to one scholar:

> These philosophical differences reflect differing historical impulses and events. In the United States, the struggle over the law of seditious libel formed an important background to the development of First Amendment law. In Germany, the totalitarian control of information by the Nazi regime formed a main motivation for the drafters of the Basic Law; they sought to guarantee broad expression and informational rights as a means to prevent any recurrence of totalitarianism.[76]

The Basic Law places the highest value on human dignity, establishes numerous individual rights, and creates a structure of legal protection for those rights.[77] In order to preserve this structure, the Basic Law establishes a "militant democracy" whereby the ability of those who attempt to undermine the constitutional structure is restricted.[78] Thus, while it guarantees the protection of the rights of every individual, the Basic Law "does not grant any liberties to the enemies of

---

Germany in 1990, the East German government chose to accede to West Germany under the framework of the Basic Law, making it a document of force and permanence for a united Germany. See id.

75 See Eberle, supra note 74, at 798-99 (noting vibrancy of public discourse in contemporary Germany).

76 Id. at 801 (footnotes omitted). Similarly, the occupying powers and German drafters of the Basic Law attempted to create a stable democracy that vested limited powers in three branches of government and minimized the opportunity for small, extreme parties to gain power. See Dürig, supra note 74, at 19-20 (describing distribution of power between branches in original constitutional structure in Germany).

77 The very first section of the Basic Law states: "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority." Grundgesetz [Constitution] [GG] art. 1(1) (F.R.G.), translated in 6 Constitutions of the Countries of the World 106 (Albert P. Blaustein & Gisbert H. Flanz eds., 1994) [hereinafter Constitutions of the World]. The Federal Constitutional Court has upheld this primacy, describing the "dignity of man" as the "center of all [the Basic Law's] determinations." See Entscheidungen des Bundesverfassungsgerichts [BVerfGE] [Federal Constitutional Court] 39, 1 (67) (F.R.G.), quoted in David E. Weiss, Striking a Difficult Balance: Combatting the Threat of Neo-Nazism in Germany While Preserving Individual Liberties, 27 Vand. J. Transnat'l L. 899, 918 (1994). The focus on the rights of the individual and the protection of the dignity of the citizenry is a departure from previous governing structures in Germany's history and is a direct reaction to Hitler's dictatorial regime. See Dürig, supra note 74, at 15 (noting that Basic Law has "incomparably strengthened the rights of the individual"). This contrasts sharply with the above outlined theories on America's participatory democracy that are grounded in part on the free flow of ideas. See supra Part I.A.

78 This structure is established in Article 2, which reads: "Everybody has the right to self-fulfillment in so far as they do not violate the rights of others or offend against the constitutional order or morality." Grundgesetz [Constitution] [GG] art. 2(1), translated in Constitutions of the World, supra note 77, at 106.

liberty."[79] Basic rights, including the right to free speech, can therefore be trumped if their exercise is seen as a threat to the fundamental constitutional structure itself.

Rights enshrined in the Basic Law can be limited in two broad ways: through other constitutional provisions or through general laws.[80] The Basic Law establishes an enforceable hierarchy of rights, and the Constitutional Court weighs constitutional limitations when rights conflict.[81] General laws passed by state or federal governments may also restrict rights,[82] though the legislature is obliged to inquire whether an infringement of the free democratic basic order could be established through its legislation.[83] To be limited and therefore constitutional, a law needs to satisfy two requirements: (1) the law must be content neutral (i.e., must regulate matters rather than ideas), and (2) the law may limit individual liberty only if the purpose of the law has a higher rank of importance than the individual liberty itself.[84]

Through the balancing of constitutional rights, Germany can restrict basic freedoms in order to safeguard the public peace,[85] to legis-

---

79 Dürig, supra note 74, at 16. For example, there are restrictions on rightist political parties and on those that do not receive over a certain percent of the vote. See Grundgesetz [Constitution] [GG] art. 21(2), translated in Constitutions of the World, supra note 77, at 115.

80 See Eberle, supra note 74, at 802 & n.11 (explaining "general law exception" and distinguishing it from American concept of First Amendment content neutrality). Moreover, liberties can be limited if they infringe on the "right to personal respect." Grundgesetz [Constitution] [GG] art. 5(2), translated in Constitutions of the World, supra note 77, at 107. See also Kommers, supra note 74, at 857 (describing role of personal honor provision of Basic Law in Constitutional Court decisionmaking).

81 See Kommers, supra note 74, at 857 (explaining that even rights framed in unconditional language are not absolute when in conflict). For example, Article 18 provides for the forfeiture of certain rights if those rights are used "to undermine the free democratic basic order." Grundgesetz [Constitution] [GG] art. 18, translated in Constitutions of the World, supra note 77, at 113-14. The Constitutional Court, which has jurisdiction limited to issues related to the Basic Law, see Kommers, supra note 74, at 840 (describing Constitutional Court as "specialized constitutional tribunal"), passes upon the validity of challenged legislation and nullifies laws that do not meet strict constitutional requirements. See Karl Doehring, The Special Character of the Constitution of the Federal Republic of Germany as a Free Democratic Basic Order, in The Constitution of the Federal Republic of Germany, supra note 74, at 25, 25 (noting power of Constitutional Court to issue decisions that bind legislature).

82 See Grundgesetz [Constitution] [GG] art. 5(2), translated in Constitutions of the World, supra note 77, at 107. See generally Weiss, supra note 77 (analyzing German laws restricting individual liberties in order to combat neo-Nazism).

83 See Doehring, supra note 81, at 33 (detailing legislature's duty to uphold "free democratic order").

84 See Grundgesetz [Constitution] [GG] art. 5(2), translated in Constitutions of the World, supra note 77, at 107 ("These rights are subject to limitations embodied in the provisions of general legislation, statutory provisions for the protection of young persons[,] and the citizen's right to personal respect.").

85 See Strafgesetzbuch [Penal Code] [StGB] § 30 (F.R.G.).

late against the crime of insult,[86] and to restrict the defamation of a deceased person.[87] While these examples may not be entirely foreign to the American legal landscape, the Basic Law's militant democracy allows restrictions that are not possible in the United States. For example, Article 131 of the German Penal Code, entitled Protection of the Public Peace, prohibits any writing or broadcast that incites racial hatred or "describe[s] cruel or otherwise inhuman acts of violence against humans in a manner which glorifies or minimizes such acts."[88] Other restrictions that are rooted in Germany's historical experience are strict bans on Nazi propaganda, the Hitler salute, and other symbols associated with the Nazi regime.[89]

While freedom of speech in Germany is enshrined in the Basic Law,[90] specific constitutional provision is made for the abridgment of speech that furthers the militant democracy goals outlined above.[91] Because of this balance and the precautionary underpinnings of the

---

[86] See id. § 185. This provision is intended largely to combat denials of the Holocaust. See Eric Stein, History Against Free Speech: The New German Law Against the "Auschwitz"—and Other—"Lies," 85 Mich. L. Rev. 277, 286-87 (1986) (detailing history of crime of insult).

[87] See StGB § 194(2).

[88] Id. § 131, translated in Stein, supra note 86, at 323. Current events and historical reports are exempted. See Stein, supra note 86, at 285 (detailing specific exemptions from prohibitions against extremist violence). Another example is the limits on political activity that would be impossible in the United States but are applied in Germany, such as the ban on political parties that are deemed to threaten the free democratic basic order. See Grundgesetz [Constitution] [GG] art. 21(2), translated in Constitutions of the World, supra note 77, at 115.

[89] See StGB § 86(I)(4) (prohibiting dissemination of goods used to propagate Nazi ideology); see also Weiss, supra note 77, at 928 (noting that Basic Law and criminal code provisions grant German courts broad discretion to restrict Nazi propaganda). Prohibitions on rightist propaganda are continually being updated and expanded. For example, a recent law was passed that outlaws the denial of the existence of the Holocaust. See Marjorie Miller, German Ban on Holocaust Denial Upheld, L.A. Times, Apr. 27, 1994, at 7 (quoting statement of Constitutional Court Justice Dieter Grimm that "'proven untruthful statements do not have the protection of freedom of speech'").

[90] Article 5(1) provides:

> Everybody has the right freely to express and disseminate their opinions orally, in writing or visually and to obtain information from generally accessible sources without hindrance. Freedom of the press and freedom of reporting through audiovisual media shall be guaranteed. There shall be no censorship.

Grundgesetz [Constitution] [GG] art. 5(1), translated in Constitutions of the World, supra note 77, at 107.

[91] See id. art. 18, translated in Constitutions of the World, supra note 77, at 113-14 ("Those who abuse their freedom of expression . . . in order to undermine the free democratic basic order shall forfeit these basic rights."). Limits on free speech thus hinge on whether the speech threatens the "'free democratic basic order,'" a concept that generally means "the liberal democracy consciously created, promoted, and protected by express provisions of the Basic Law." Donald P. Kommers, The Jurisprudence of Free Speech in the United States and the Federal Republic of Germany, 53 S. Cal. L. Rev. 657, 680 (1980) (citation omitted).

Basic Law,[92] extremist political speech is the primary concern of German policymakers, while indecent sexual materials present less of a concern.[93] The next section analyzes how these different priorities have played out in Germany's legislative Internet content regulation.

2. *German Internet Regulation*

While Internet use is not as widespread in Germany as in the United States,[94] Internet regulation in Germany has been a "particularly prickly" issue.[95] In contrast to the net-friendly United States, Germany has been called one of the most Internet-averse nations,[96] due in large part to aggressive use of laws prohibiting extremist propaganda and pornography to keep the Net clean.[97] In a now infamous

---

92 See supra notes 74-79 and accompanying text (detailing theoretical basis of Basic Law's free speech protections).

93 See Mary Williams Walsh, 2 Views on 1st Amendment: As Americans Decry What They See as Online Censorship, Germans Wonder What All the Fuss is About, L.A. Times, Mar. 13, 1996, at D5 (noting that restrictions on certain sexual expression are "viewed as a weird, even ridiculous phenomenon," though "Germans tolerate state intrusions that many Americans would fight as overarching Big Brotherism"). However, Germany does have proscriptions against child pornography and hard-core obscene materials similar to those of the United States. See id. (noting generally more liberal attitude towards sexual materials, but conceding that Germany has strict prohibitions on child pornography and other hard-core obscenity).

94 In 1996, only two percent of Germans reported using the Internet at home or work, and over three-quarters said they have never heard of the Internet. See A Land of New Media Apathy, New Media Age, Aug. 1, 1996, at 8, available in Lexis, News Library, Nmdage File (comparing Internet use statistics among Germany and other nations).

95 Andrew Gray, Germany Plans Bill to Punish Internet Indecency, Reuters North American Wire, Mar. 29, 1996, available in Lexis, News Library, Reuna File.

96 See, e.g., Brandon Mitchener, Ex-CompuServe Official Convicted in German Court, Wall St. J., May 29, 1998, at B7 (stating that German online prosecutions give Germany "'a black eye in the Internet field'" (quoting Christopher Kuner, attorney for ISP defendant)); Hans-Werner Moritz, Pornography Prosecution in Germany Rattles ISPs, Nat'l L.J., Dec. 14, 1998, at B7 (noting that recent prosecution of ISP executive for Internet-related offense "sent shock waves through the German high-tech industry and again illustrated how advancing technology strains well-established legal concepts"); Walsh, supra note 93, at D5 ("When it comes to free speech, Germany ranks right up there with the Iranian mullahs—or so it seems to Internet enthusiasts horrified by the eagerness of governments in the U.S. and around the world to censor the nascent medium.").

97 Germany's concerns about hate speech on the Internet are echoed by other member states of the European Union (EU). For example, the EU Consultative Commission on Racism and Xenophobia urged member states to "take all needed measures to prevent [the] Internet from becoming a vehicle for the incitement of racist hatred." Knoll, supra note 54, at 286 (citation omitted). Commission members likened the directive to previous calls to limit television broadcasting that incited racial hatred and remarked that they did not want to chill free expression. See id. at 286-87 ("The Consultative Commission noted that it did not want to interfere with free speech, but that Commission members had discussed 'racism in cyberspace' and harkened to earlier EU directives in which the EU had urged Member States 'to shun television programmes which incited hatred on grounds of race, sex, religion or nationality.'" (citation omitted)).

1995 incident, CompuServe blocked access to 200 chat groups for fear of prosecution under Bavaria's obscenity laws.[98] Because CompuServe did not have the technology to ban the groups only to its 220,000 customers in Germany, it had to ban the groups worldwide, suspending access to four million subscribers in 147 countries.[99] The ban occurred after Internet-surfing police in Munich executed a search warrant on CompuServe's Munich office in connection with a government probe of online pornography.[100] While the prosecutor denied pressuring CompuServe into compliance, CompuServe stated it had no choice but to shut down the sites, despite pressure from customers to resist censorship.[101]

Munich prosecutors followed with charges that CompuServe general manager Felix Somm was an accessory to the dissemination of pornography and extremist propaganda, alleging that customers had access to forbidden images of Hitler and Nazi symbols.[102] Somm did not deny that those who break existing laws should be prosecuted, but argued that CompuServe was like a telephone company which cannot be held liable for criminal conversations that occur over their lines.[103] Munich prosecutors initially argued that CompuServe could have installed software suitable for blocking objectionable news groups to keep objectionable material from customers.[104] They noted that America Online Germany and the Microsoft Network had built-in technology that could allow parents to control what their children could reach on the Internet.[105] CompuServe subsequently offered similar software that allowed parents to block out objectionable mate-

98 See Moritz, supra note 96, at B7.

99 See Knoll, supra note 54, at 287 (discussing subscribers affected by temporary worldwide ban); Kara Swisher, Cyberporn Debate Goes International: Germany Pulls the Shade on CompuServe, Internet, Wash. Post, Jan. 1, 1996, at F13 (same); Walsh, supra note 93, at D5 (same). See generally infra Part III (describing technological solutions employed by CompuServe to internalize German legal restrictions).

100 See Moritz, supra note 96, at B7.

101 See Knoll, supra note 54, at 287 (discussing denial by Munich's senior public prosecutor); Walsh, supra note 93, at D5 (outlining "angry" reactions by Internet activists). The Bavarian incident provides perhaps the best example of "lowest common denominator" regulation in which a local regulation effectively denied access to Internet content worldwide.

102 See Walsh, supra note 93, at D5. The Somm prosecution was one of the first successful prosecutions of an ISP official for objectionable online content and received significant media attention. See, e.g., Moritz, supra note 96, at B7.

103 See Moritz, supra note 96, at B7 (describing CompuServe as not liable under German law because it is "a mere provider of access to third-party content").

104 See id.

105 See id.

rial.[106] Despite these efforts to ameliorate German concerns, prosecutors indicated that CompuServe could be held liable if they found such news groups again in Germany.[107]

A number of similar incidents occurred that caused concern among many ISPs about potential liability for content under Germany's laws. For instance, prosecutors in Mannheim investigated CompuServe and Deutsche Telekom AG's T-Online service because users could access a Canadian neo-Nazi site on the World Wide Web.[108] Public and industry reaction around the world to Germany's strict policing of online content largely was negative.[109] Regardless, Germany, reflecting its significant concern about extremist online propaganda and relatively limited constitutional protection of free speech, enacted Europe's first comprehensive Internet content control legislation in 1997.[110] The Information and Communication Services Act (ISCA)[111] has three main effects on Internet content in Germany. First, the law subjects ISPs to criminal prosecution for knowingly acting as a conduit for illegal content that is technically possible to halt in transmission.[112] Second, the ISCA requires that ISP offices have bu-

---

106 See id. (discussing CompuServe's decision to offer blocking technology to individual users). It is this sort of technological, rather than legislative, solution to Internet content control that this Note advocates. See infra Part III.

107 See Knoll, supra note 54, at 288. Somm was convicted of spreading pornography via the Internet in May, 1998. See Mitchener, supra note 96, at B7 (reporting Somm conviction).

108 See Walsh, supra note 93, at D5.

109 See, e.g., Moritz, supra note 96, at B7 ("Public reaction to the newsgroups' suspension was overwhelmingly negative."); Sylvia Dennis, Int'l Civil Liberties Groups Protest CompuServe Prosecution, Newsbytes News Network, Apr. 24, 1997, available in 1997 WL 10171799 (stating that Somm prosecution "upset German and other country civil liberties groups to the extent that they have banded together to lobby the German government over the affair"); New Media, Comm. Daily, Apr. 24, 1997, available in 1997 WL 3943891 (noting coalition of 23 Internet groups' protest letter to Chancellor Kohl about Somm prosecution).

110 See Steve Gold, German Gov't Plans to Police the Internet, Newsbytes News Network, Apr. 21, 1997, available in 1997 WL 10171521 (noting "the Information and Communications Service Bill . . . proposes that anyone transgressing Germany's laws, notably those relating to pornography or prohibited subjects, such as the Reich, Hitler glorification, and Neo-Nazi topics, will be subject to 'swift legal retribution'"). Supporters of the Act argued that Nazi propaganda and extremist speech on the Internet warranted unilateral government control. Then-Technology Minister Jürgen Rüttgers stated simply, "The Internet must not become a legal vacuum. This country is not prepared to tolerate certain things that appear there." Id. While the opposition Social Democrats said that trying to censor the Internet would fail, they nonetheless called for a police-run national coordination center to monitor illegal online activities. See id.

111 Informations und Kommunikationsdiesnte-Gesetz [Information and Communication Services Act] [IuKDG] (F.R.G.) (visited Mar. 2, 1999) <http://www.iid.de/rahmen/iukdge.html>.

112 See id. art. 1, § 5(2) ("Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are

reaucrats, or "Youth Protection Officers," to troll the Internet for objectionable material.[113] Third, the ISCA makes it a crime to disseminate or make accessible materials deemed harmful to children.[114]

Though aggressive prosecution and restrictive legislation such as the ISCA allow Germany to pursue its policy goals online, there are significant costs to a strict legislative approach to content control. Upon passage of the ISCA, critics felt it was too stringent and would stall growth of Internet use in Germany.[115] Some business leaders thought that such legislative Internet regulation could deter technological investment in Germany.[116] The German Chamber of Industry and Commerce said that the measures that held ISPs responsible for material posted by a third party would place German business at a disadvantage relative to U.S. companies.[117] Indeed, the excessive regulatory environment perceived in Europe may threaten the nascent Internet industry there. "People in Europe still underestimate the significance of electronic commerce for business, the working environment and the consumer," said German Economics Minister Guenther Rexrodt.[118] For the full benefits of the Internet to be realized, Germany must develop a way to regulate the material made available to German users without unduly burdening Internet growth in Germany or elsewhere.

II

INTERNET REGULATORY REGIMES

As a threshold issue, it is essential to recall that, given domestic political concerns and legal constraints in the United States and Ger-

technically able and can reasonably be expected to block the use of such content."). Note that, as in the United States, technological solutions to avoid governmental regulation are explicitly presented as a safe harbor from government censorship. See id.; see also infra Part III for a further explanation of how such alternatives could operate to avoid unilateral government censorship altogether.

113 See id. art. 6, § 7(a).

114 See id. art. 6.

115 See Jordan Bonfante, The Internet Trials: Germany Makes an Early Attempt at Taming the Wide, Wild Web, Time Int'l, July 14, 1997, at 30, available in 1997 WL 10902596 (outlining criticism).

116 See id. (noting that new law could "drive away foreign investment in the high-tech industry that Germany needs most to develop").

117 See Matt Marshall, Germany Silently Accepts U.S. Internet Trade Plan, Wall St. J. Eur., July 8, 1997, at 3, available in 1997 WL-WSJE 12207977.

118 U.S. Urges Europeans to Go Easy on Internet Regulation, Dow Jones News Service, July 7, 1997, available in Westlaw, ALLNEWSPLUS database.

many, the Internet cannot be a wholly unregulated medium.[119] The question, then, is not whether, but how, Internet content is regulated: publicly through legislation, or privately through technology- and market-based solutions. This section outlines available regulatory mechanisms in order to understand which method is least restrictive within the context of legal necessities in different countries. It begins with a discussion of how informal self-regulation failed to allay concerns over Internet content effectively and fed a perceived need for legislative content regulation. Next, three types of Internet regulation are examined: firewalls, legislation against specific content, and market regulation.

A. Necessity of Regulation

Early in its development, Internet content was regulated informally. A so-called "nettiquette" developed in which objectionable material, such as foul language, was censured by other Internet users who came across the content.[120] For example, a user who received an objectionable and unsolicited e-mail would respond to the sender by "flaming"—that is, sending an insulting response in all capital letters.[121] More drastically, computer-savvy users could "spam" the violator, or overload his or her computer with useless information or repetitive messages.[122] At this point, Internet use was not widespread and the vast majority of users were adults (scientists, military personnel, and academics) who could regulate content by simply not accessing chatgroups or web pages that they found undesirable.[123]

As the number of Internet users grew and the medium became more inclusive, this informal method of regulation was increasingly seen as inadequate.[124] Further, technological advances enhanced the

---

119 See supra Part I (arguing that political pressures lead U.S. policymakers to be concerned with children accessing sexually explicit material, while German authorities look to cut off certain banned political speech altogether).

120 See Greenlaw & Hepp, supra note 2, § 2.5.2, at 37; see also Robert L. Dunne, Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm, 35 Jurimetrics J. 1, 10-11 (1994) (discussing early efforts to regulate Internet through imposition of norms of behavior); Ilene Knable Gotts & Alan D. Rutenberg, Navigating the Global Information Superhighway: A Bumpy Road Lies Ahead, 8 Harv. J.L. & Tech. 275, 278 n.19 (1995) (describing early Internet self-regulation).

121 See Greenlaw & Hepp, supra note 2, § 2.5.2, at 37. Capital letters are used to signify that the writer is shouting. Alternatively, a user could censure an objectionable message by sending a known symbol of disapproval to the original sender. For example, the upside down frown, :-(, seen by turning the page sideways, conveys disapproval. See id.

122 See id. § 2.2.3, at 18.

123 See Dunne, supra note 120, at 11 (noting common understanding among early Internet users).

124 See, e.g., id. (arguing that time had come for "informal way of doing things on the frontier" to give way to regulation); I. Trotter Hardy, The Proper Legal Regime for

potential for offensive materials to be seen online, as mischievous users could add objectionable pictures and even moving images to what was previously only text. Despite these developments in the Internet and its use, some argue that an informal system of self-regulation can still effectively police the Internet and that government regulation of content should be disallowed altogether. So-called "cyberlibertarians," such as John Perry Barlow of the Electronic Frontier Foundation, argue that the Internet is an entirely new technology not amenable to content control, and that any regulation is antithetical to free speech.[125]

This conception of the Internet as a regulation-free medium, while highly appealing in principle, is not a viable system. Informal regulation, for example, cannot prevent people who prey on children from disseminating sexually explicit ideas and materials,[126] nor can it prevent children from mistakenly accessing inappropriate websites. Further, governments will be unlikely to support a system whereby communications over the Internet that violate national laws are immune from scrutiny.[127] Perhaps most importantly, informal regulation is not politically viable. As explained in Part I, political pressures in the United States to curb sexually graphic materials and protect children will not be appeased by a purely self-regulatory approach. Similarly, historical circumstance in Germany has led to the prohibition of certain forms of political speech that will not be tolerated in any medium, including the Internet.[128] The adoption of informal regulation alone could result in a political backlash leading to excessively rigid

---

"Cyberspace," 55 U. Pitt. L. Rev. 993, 1026-28 (1994) (suggesting that this type of self-help is effective for some discussion group conflicts, but not as effective for major concern of pornography).

[125] Barlow describes the new territory of cyberspace in eloquent terms:

> You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity—from the debasing to the angelic—are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

John Perry Barlow, A Declaration of the Independence of Cyberspace, The Humanist, May/June 1996, at 18. Barlow and others would also exempt the Internet from other existing laws, such as copyright, arguing that "because copies do not deprive authors of their originals, they should be as free as the air." Dan Rosen, Surfing the Sento, 12 Berkeley Tech. L.J. 213, 215-16 & n.13 (1997) (citing Barlow's remarks at digital content conference, University of California at Berkeley, Nov. 8, 1996).

[126] See Spiliopoulos, supra note 20, at 359.

[127] Germany, for example, would not accept a system whereby its antipropaganda laws, such as the one involved in Dagmar's hypothetical, see supra text accompanying notes 5-6, could not be enforced online.

[128] See supra Part I.B (describing restrictions on certain political speech in Germany).

legislative content regulation. The situation has been aptly described by Professor Lessig:

> [I]f Congress is not likely to let things alone (or at least if the President is more likely to bully a "private solution" than leave things alone) then we need to think through the consequences of these different solutions. . . . However much we prefer that nothing be done, whether through public or private regulation, we should reckon its consequences for free speech, and choose the least burdensome path.[129]

B. Regulatory Options

1. Firewalls

Perhaps the most burdensome type of regulation, national "firewalls" allow governments to regulate the Internet strictly by censoring information as it crosses national borders.[130] Firewalls operate by having government censors stall content in transmission, making it available to citizens only after it has been scanned for undesirable content.[131] For example, the Chinese government created a firewall around the entire country's computer networks in 1996 when it implemented strict Internet access regulation.[132] The regulations require "Internet service providers to use only government-provided phone lines and to register with the police."[133] The Chinese government did not stop with provider-side regulation but also required users to "register with the police, and sign a pledge not to 'harm' China's national interests."[134] All Internet traffic is routed through two gateways in Beijing and Shanghai, where police monitor transmissions and block access to specific banned sites, including sites of many foreign newspapers and human rights groups.[135]

---

129 Lessig, supra note 1, at 633.

130 See John T. Delacourt, Recent Development, The International Impact of Internet Regulation, 38 Harv. Int'l L.J. 207, 215-16 (1997) (describing national firewalls).

131 See id.

132 See id. (describing Chinese efforts to regulate Internet content through national firewall); Erik Eckholm, China Cracks Down on Dissent in Cyberspace, N.Y. Times, Dec. 31, 1997, at A3 (discussing new Chinese restrictions on use of Internet to "defame Government agencies, to promote separatist movements or to divulge state secrets"); Testing the Boundaries, Countries Face Cyber Control in Their Own Ways, L.A. Times, June 30, 1997, at D1 [hereinafter Testing the Boundaries] (detailing specific requirements for Internet use in China, and calling China "[t]he most Draconian of all Net regulators").

133 Testing the Boundaries, supra note 132, at D1.

134 Id.

135 See id. Similarly, ISPs in Singapore are regulated by the Singapore Broadcasting Authority and must adhere to the agency's strict restrictions on "objectionable" content, which limit pornography and materials that challenge "public morals, political stability, and religious harmony." Id.

There are a number of problems with censorship through firewalls. First, such programs may not be technologically feasible because the Internet is far too vast to be effectively policed on a national scale.[136] The Chinese have addressed this problem by limiting the number of citizens licensed to use the Internet,[137] a policy that is unlikely to survive in more market-oriented economies like those in the United States and Germany.[138] Second, even if feasible, blocking transmission at a country's borders in order to check all incoming content would delay transmission and increase costs of Internet service significantly.[139] Third, firewalls are neither narrowly tailored nor the least restrictive means of regulation, conditions necessary to pass constitutional muster in the United States.[140] Finally, a country's effort to stop all digital traffic at the border underestimates the ability of knowledgeable Internet "surfers" to reroute transmissions around government firewalls and access off-limits information.[141] In sum, firewalls misapprehend Internet technology and prevent the development of the Internet as an informational and economic tool.[142]

---

136 See Delacourt, supra note 130, at 215-16 (describing Chinese efforts to monitor "influx of outside information" over Internet); Peter H. Lewis, Limiting a Medium Without Boundaries, N.Y. Times, Jan. 15, 1996, at D1 (detailing difficulties of policing global Internet with national monitoring regimes).

137 Only an estimated 150,000 people use the Internet in China, and Beijing, the center of China's Internet industry, has only 20 ISPs. See Testing the Boundaries, supra note 132, at D1. Further, the Chinese authorities attempt to limit Internet use to certain professions. See Delacourt, supra note 130, at 216; Steve Mufson, China Opens a Window on Cyberspace, Wash. Post, June 19, 1995, at A1 (reporting impact of Internet on Chinese efforts to eliminate political dissent). China also keeps the cost of Internet service artificially high to discourage use. See Internet Poses a Problem in Asia, S.F. Chron., May 29, 1995, at A14 (discussing efforts of Chinese authorities to restrict Internet access to more easily controlled few).

138 See Delacourt, supra note 130, at 216 (arguing that, "to the extent [such monitoring measures] succeed and access to the Internet is limited, any economic development attributable to the Internet is correspondingly minimized").

139 See Ari Staiman, Shielding Internet Users from Undesirable Content: The Advantages of a PICS-Based Rating System, 20 Fordham Int'l L.J. 866, 904-05 & n.330 (1997) (discussing costs of "stall and scan" approach to Internet regulation).

140 See supra notes 65-66 and accompanying text (outlining reasoning for invalidation of CDA).

141 See Dunne, supra note 120, at 10-11 (discussing hackers who specialize in accessing off-limits material). The Internet began as a United States Department of Defense initiative to decentralize computer communication in the event of a nuclear attack, see Clark, supra note 2, at 5, and firewalls are just the sort of barriers the system was intended to allow users to avoid.

142 Note, however, that these criticisms do not rule out a system in which a country could impose its own standards by focusing on the *user* rather than the transmission or the service provider. See infra Part III (arguing that governments could require software to be installed on users' computers to block illegal material that has been previously rated).

2. *Legislation Against Specific Content*

Legislation against certain Internet content is used widely to protect users and others from content that is illegal under domestic laws.[143] Such regulation focuses on removing a certain site or type of site from the Internet on a piecemeal basis after it enters a country. Because the removal of illegal content is less extreme and cheaper than firewalls, most Western nations, including the United States and Germany, have adopted some form of selective regulation of illegal sites as the favored method of regulation.[144]

Unilateral removal of content, however, has three main difficulties as a regulatory regime. First, as in the United States, some material (such as sexually explicit images) may be legal but deemed inappropriate for certain people, such as children. A unilateral removal of such material would lead to overregulation and would chill the free flow of ideas on the Internet.[145] For example, legislation such as COPA that outlaws material harmful to minors could completely ban such materials rather than restrict them on a case-by-case basis. Regardless of one's personal opinion of pornography, banning all such material violates the constitutional rights of adults to access it.[146]

Second, jurisdictional difficulties often preclude prosecution for the violation of domestic law by a foreign content provider or ISP. For example, an American writer who publishes some gossip about a British citizen on the Internet may have violated Britain's more stringent libel laws but has committed no offense in the United States.[147]

---

143 See Staiman, supra note 139, at 905 (describing, by example, application of existing laws to Internet); Testing the Boundaries, supra note 132, at D1 (surveying international Internet content control through existing legislation).

144 See supra Part I.A.2 (discussing U.S. Internet regulation); supra Part I.B.2 (discussing German Internet regulation). Japan and many European countries also employ this regulatory method, at least in part. See Testing the Boundaries, supra note 132, at D1 (noting application of legislation in Japan and France); Banned President Mitterand Book Posted Online, Newsbytes News Network, Jan. 25, 1996, available in Westlaw, NEWSBYTE file (noting French government effort to ban Mitterand biography from Internet). In addition to the application of existing laws, see, e.g., supra notes 43-49 and accompanying text (detailing *Thomas* conviction under general obscenity law), a country could exert economic pressure on foreign ISPs to force them to comply with censors. A government could take action against an ISP's property or assets in the country if the ISP provided access to users through non-governmentally controlled channels. For example, Chinese officials banned the satellite dishes of a satellite television company that sent objectionable material from Turkey to Japan that incidentally crossed China. See Delacourt, supra note 130, at 215-16 (recounting Chinese efforts to control technology that crosses its airspace).

145 See, e.g., Reno v. ACLU, 117 S. Ct. 2329, 2343-44 (1997) (discussing "obvious chilling effect on free speech" of content-based regulation).

146 See supra notes 32-38 and accompanying text (discussing "indecent" materials).

147 See Kyu Ho Youm, Suing American Media in Foreign Courts: Doing an End-Run Around U.S. Libel Law?, 16 Hastings Comm. & Ent. L.J. 235, 239-44 (1994) (comparing American and English libel laws).

It would be impractical to hold the ISP liable for unknowingly transmitting the website to a user in England, and, in any case, the ISP may be foreign-based as well. Moreover, a regulatory system that subjects ISPs to the jurisdiction of any nation in which they operate would lead to a form of "lowest common denominator" regulation in which ISPs cater to the laws of the country with the most stringent content requirements.

Third, Internet technology allows a content provider to mask the origin of material through rerouting and anonymous remailing.[148] This leaves only the ISP as a potentially liable party for the content, which raises the same jurisdictional and lowest common denominator difficulties discussed above. In sum, the current system of legislation against specific content on the Internet is not a viable solution to objectionable content. Instead, the failures of the system indicate that any solution must be international in nature while simultaneously decentralized enough to allow nations to apply their domestic laws to the Internet effectively.

3. *Market-Based Regulation*

While firewalls and specific pieces of legislation focus on "top-down" government regulation, alternatives have developed that focus not on what a user is offered on the Internet, but rather on what a user may retrieve.[149] Such alternatives benefit from being decentralized to the user's computer or a network of computers, and therefore are more flexible and can be tailored to specific regulatory goals. Because some regulation of the Internet is inevitable and the existing regimes outlined above are less than ideal, technology-based proposals that focus on systematically rating certain Internet material are the most promising alternatives to avoid government censorship.[150]

A market-based decentralized regulatory regime would be founded on the filtering of unwanted materials from a specific user's

---

148 See W. John MacMullen, Anonymity, Privacy, and Security, in Internet Issues and Applications, 1997-1998, at 67, 75-79 (Bert J. Dempsey & Paul Jones eds., 1998) (describing remailing technology).

149 See, e.g., Amy Harmon, Technology to Let Engineers Filter the Web and Judge Content, N.Y. Times, Jan. 19, 1998, at D1 (describing filtering technology). Note that decentralized market-based approaches may not satisfy the most stringent Internet censors such as China, which would want to purge the Internet of certain materials altogether. However, market-based regulation, supplemented by the implementation of existing laws to the Internet, would satisfy regulatory pressures in the United States, Germany, and other Internet-friendly nations. Further, the continued imposition of firewalls in China would not have extraterritorial effect on Internet viewers in other nations.

150 See Delacourt, supra note 130, at 224-34 (outlining support for alternative regulation of Internet content, based on ratings and screening software); Staiman, supra note 139, at 869 (arguing for adoption of ratings template by EU).

computer. The system would have two components: (1) a rating system, and (2) screening software that can identify the ratings and block certain material. The Internet already employs various forms of rating. For example, many web pages that contain sexually explicit or violent material are preceded by a warning message that appears on the user's computer screen.[151] Online service providers also have monitored chat rooms to assure that content is appropriate for children.[152] Further, many ISPs, acting out of liability concerns as well as the desire to avoid unilateral regulation, have rated content by developing "blacklists" of sites that they determine to be obscene or otherwise offensive.[153]

Blacklists and monitoring by ISPs, however, are cumbersome technologies that suffer from serious concerns about overregulation and the imposition of someone else's morality on an unsuspecting viewer.[154] Further, it is impossible for an individual ISP to review all the content offered on the Web.[155] While some providers have resorted to word searching and screening on the basis of objectionable phrases, such a regime is not functional in practice.[156] Moreover, blacklists may not be effective because they only ban the *address*, not the content itself, and Internet technology allows another content provider or user to circumvent this restriction by simply placing the content on another address.[157]

Though such initiatives are flawed, they indicate an important factor in constructing viable ratings and software technology: The Internet industry has an inclination to participate in a system of market-

---

151 See Delacourt, supra note 130, at 225. Of course, such restrictions, with nothing further, fall prey to the concerns outlined above regarding informal Internet content control. See supra Part II.A.

152 See Johnson, supra note 41, at 87 & n.130 (citing Prodigy's claim that it is "family oriented computer network" that exercises editorial control over messages posted on its bulletin boards).

153 For example, CompuServe maintains a blacklist of addresses that its "reviewers" have deemed inappropriate as part of the software package that they market to consumers in the U.S. and elsewhere as "child-friendly." See id. at 87 n.130 (describing efforts by Prodigy and CompuServe to block content that is not "family-oriented"); see also Netscape Unveils Smart Browsing, M2 Presswire, June 2, 1998, available in 1998 WL 12209267 (discussing screening component of Netscape's new browser which allows users to screen for adult language, violence, and nudity).

154 See Amy Harmon, The Self-Appointed Cops of the Information Age, N.Y. Times, Dec. 7, 1997, § 4, at 1 (noting that "[s]ome parents might disagree with [ratings] choices, if they knew what was excluded").

155 See id. ("Since the Web is so big, with hundreds of cites added daily, much of the material is blocked simply because software monitors have not had time to review it.").

156 See id. (outlining problems with blacklists and keyword blocking); infra note 176 and accompanying text (detailing America Online's screening out all content with word "breast," thus denying access to chatrooms and information about breast cancer).

157 See Staiman, supra note 139, at 881 (describing address-based restrictions).

based regulation.[158] In the United States, "the well-funded U.S. [Internet] industry has organized itself around a common goal: keeping national governments out of Internet regulation."[159] Industry efforts are global as well. Early in 1999, a worldwide group of over 100 media and telecommunications companies launched an organization aimed at ensuring "that the [I]nternet is self-regulated on a global basis, rather than being left to national governments."[160] The success of such efforts to preempt legislative regulation depends on the availability of an internationally standardized system for ratings and software that provides incentives for various companies and organizations to participate. A number of initiatives have already been launched, including one by the Internet Services Association (ISA), a nonprofit association comprised of ISPs.[161] A more ambitious proposal, the Platform for Internet Content Selection (PICS), is an international effort to harmonize ratings of different bodies so that various screening software packages can detect and block material according to national laws or user needs. A proposal like PICS is a promising alternative that would allow each country, including the United States and Germany, to pursue its policy goals online without imposing its own legis-

158 ISPs and users would prefer to control regulatory efforts rather than acquiesce in governmental, top-down regulation of the type detailed in Part II.B.1 and 2. See Amy Harmon, Ideological Foes Meet on Web Decency, N.Y. Times, Dec. 1, 1997, at D1 (noting that online industry generally opposes legislative regulation, and rather "contend[s] that supplying parents with blocking software and rating sites . . . is more effective"). Indeed, self-regulation has proven effective for other media such as video and motion pictures, either because of "desire to avoid government regulation, or to improve the public image of the industry." Johnson, supra note 41, at 86. Note that this sort of industry (or parental) self-regulation is *not* the same as user self-regulation, see supra notes 120-23 and text accompanying notes, which refers to users policing the Internet for themselves in a non-regulatory environment.

159 Neil Munro, Who Will Rule the Net?, Nat'l J., Feb. 13, 1999, at 404. In contrast to the industry's concerted efforts to keep control of the regulatory agenda through market-based initiatives, "many of the other players with interests in the outcome—such as consumer groups, privacy advocates, unions, nationalists, and social conservatives—are scrounging for cash and arguing over problems and solutions." Id. A viable market regime that preempts the need for legislative regulation, of course, will have to internalize these other constituencies to avoid their lobbying for a greater government role.

160 John Authers, Media and Telecoms Chiefs Aim for Self-Regulation of Internet: Governments 'Should Leave Policing to Industry', Says Group, Fin. Times, Jan. 15, 1999, at 18. The group, Global Business Dialogue on E-Commerce, includes multinational companies such as IBM, MCI WorldCom, Bank of Tokyo-Mitsubishi, and France Telecom. See id.

Another international group, the Recreational Software Advisory Council (RSAC), is the leader in providing ratings labels to content providers consistent with the Platform for Internet Content Selection (PICS). See RSAC Announces Netscape Support of Recreational Software Advisory Council's Leading Internet Content Rating System, PR Newswire, June 17, 1998, available in Westlaw, ALLNEWSPLUS database.

161 The ISA proposal suggests developing technical tools for parents to screen out objectionable content. See Johnson, supra note 41, at 86 n.129.

lative regulation on the entire Internet. Such a proposal is examined in the next Part.

III
MARKET-BASED REGULATION AS THE BEST METHOD TO AVOID GOVERNMENT CENSORSHIP

The unilateral removal of content from the Internet, as practiced by the United States and Germany, is an inflexible regime that imposes one country's domestic law on a borderless medium.[162] Legislation that in effect purges information from the World Wide Web leads to overregulation, and an effective legislative regulatory structure that focused on users would curtail online privacy, a proposal that is unlikely to be accepted.[163] Moreover, holding the ISP liable for objectionable content transmitted over its wires is ineffective, creates uncertainty in regulation, and can stifle growth of the industry in a given country.[164] As one commentator observed, "[T]he legislature is not the appropriate entity to regulate the content of constitutionally protected speech transmitted by users of this rapidly developing medium."[165] This Note, in joining Professor Lessig's furious debate,[166] agrees that a decentralized technological solution, rather than legislation targeted at certain online content, is the best means to avoid "cyberanarchy."[167] Accordingly, this Part argues for a market-based

---

[162] See, e.g., Labyrinth of Laws Could Lead to a Net Loss, The Independent, Jan. 15, 1996, § 2, at 11 (arguing that country-by-country regulation leads to overregulation, as ISPs comply with most rigorous jurisdiction to avoid liability, and that international convention is necessary to determine what law should govern).

[163] Because users can navigate the Internet anonymously, a user-based regulatory regime that tracked Internet use would require users to register with their real name in order to prosecute lawbreakers. However, privacy is one of the great benefits of the Internet, see Denise Caruso, The Key Issue for the Net is Not Smut, It is the Use of Encryption, N.Y. Times, Mar. 25, 1996, at D5 (noting that restrictions on privacy could suffocate the Internet), and users would be unlikely to forego online privacy, even to avoid legislative regulation.

[164] See supra Part II (outlining problems of subjectivity in blocking, overdeterrence, inflexibility, and jurisdictional difficulties with foreign ISPs).

[165] Johnson, supra note 41, at 59.

[166] See supra note 1 and accompanying text. Basically, the debate has been between advocates of legislative regulation and supporters of technological solutions to Internet content control.

[167] Lessig is a proponent of a legislative solution:

> The 'less restrictive means' touted by free speech activists in *Reno* are, in my view, far more restrictive of free speech interests than a properly crafted CDA would be. . . . I mean to attack 'private' blocking as a solution to the 'problem' of indecency, and I mean my attack to be a constitutional one.

Lessig, supra note 1, at 632-33. See also Harmon, supra note 149, at D1 (outlining ACLU and EPIC opposition to filtering). Those arguing that the Internet can be regulated by existing laws and technological solutions include Jack L. Goldsmith, Against Cyber-

system of decentralized regulation to avoid politically expedient government censorship, a system that would place as much control as possible in the hands of individual citizens.[168] The key to such a regime is a standardized ratings system coupled with a competitive market in software packages that can internalize domestic policy goals in a decentralized regime of Internet regulation.

The different constitutional baselines in the United States and Germany serve as examples of a point largely neglected in the literature: Online regulation has to internalize vastly different legal structures as the Internet continues its fantastic global growth.[169] In both countries, the ideal baseline is no Internet-specific regulation, leaving content control to existing laws (against child pornography, libel, etc.) and screening technology. The nature of these baselines—that is, what materials are deemed objectionable by each country—is different in the United States and Germany and, indeed, varies among all nations. Screening technology, in addition to enforcing existing laws within a nation's borders, can provide the means to avoid Internet-specific legislative regulation while addressing nations' different regulatory baselines.

The technology needed to block out Internet content within an individual country while preserving full access to the rest of the World Wide Web's global subscribers already has been employed.[170] A number of software companies, including Microsoft, Net Nanny, and

---

anarchy, 65 U. Chi. L. Rev. 1199, 1200 (1998) ("[T]he skeptics underestimate the potential of traditional legal tools and technology to resolve the multijurisdictional regulatory problems implicated by cyberspace."); Staiman, supra note 139, at 918 ("The proposed global PICS-based rating system will allow each country to use the system in a way that will conform with its own laws.").

168 The Supreme Court has recognized the advantage of technology-based regulation. See infra notes 63-65 and accompanying text (detailing *Reno* Court's referencing of technological alternatives as less restrictive means than CDA's legislative strictures); see also Lessig, supra note 1, at 631 ("Let the market, let the code, let the parents, let something else make sure that porn is kept from kids. It's too early, the Court was convinced, to call in the marshal.").

169 But see Goldsmith, supra note 49, at 483-86 (discussing effects of simultaneous regulation by different jurisdictions). Generally, though, the literature about Internet content control is largely focused on the United States to the neglect of the transborder nature of Internet technology, see generally Lessig, supra note 1 (focusing on constitutional and other objections to private screening in the U.S.), or purely comparative without a proscriptive framework to internalize different countries' legal regimes, see generally Delacourt, supra note 130 (surveying U.S., German, and Chinese legal regimes); Staiman, supra note 139 (describing various countries' attempts to shield users from undesirable content).

170 See, e.g., Internet Industry's Response to Child Pornography, Nation (Newspaper), Sept. 16, 1998, available in 1998 WL 15056700 (describing PICS and other initiatives); supra notes 105-06 and accompanying text (detailing CompuServe's use of technology to block 200 objectionable newsgroups in Germany to avoid threat of prosecution).

Solid Oak Software, have developed control filters for the Internet,[171] indicating the presence of a nascent competitive market in software packages. These products allow parents or online users to control content by customizing the software filter used when they access the Internet. Generally, such software can block access to the World Wide Web, newsgroups, and other online services, and can allow a parent to prohibit access on particular days of the week or particular times of the day.[172] ISPs like Prodigy, America Online, and Microsoft Network also offer options free of charge that allow subscribers to control what children can access online.[173] In addition to such services, software programs are available that can screen content by word or phrase (e.g., "sex" or "neo-Nazi") and maintain tailored lists of sites known to contain objectionable materials.[174] Sometimes, however, such efforts are cumbersome and suffer from a lack of standardization because each relies on its own method of rating.[175] For example, in 1995, America Online screened out material with the word "breast," thereby denying access to information and discussion groups about breast cancer.[176]

A standardized template for ratings could allow different countries and different users (i.e., parents, schools, and libraries) to employ various ratings systems to selectively screen those materials deemed objectionable.[177] In conjunction with the software described above,

---

171 See Diane Roberts, On the Plurality of Ratings, 15 Cardozo Arts & Ent. L.J. 105, 117-18 (1997) (detailing parental control filters for Internet); Filtering Software Will Likely Be in Spotlight with Summit, Dow Jones Online News, Nov. 26, 1997, available in Westlaw, ALLNEWSPLUS database (noting different types of filtering software).

172 See Roberts, supra note 171, at 118.

173 See Spiliopoulos, supra note 20, at 358.

174 See id. (describing software programs such as Cyber Patrol and SurfWatch).

175 Because there are as many rating systems as there are screening software programs, ratings are not standardized and therefore not clear or easily applied. These problems can be addressed by a standardized template that can read various web page ratings, as described infra notes 185-91 and accompanying text (describing PICS-compliant ratings systems).

176 See Amy Harmon, On-Line Service Draws Protest in Censor Flap, L.A. Times, Dec. 2, 1995, at D1. This incident, in which an ISP blocked all references to a word on its network blacklist, see supra notes 153-54 (describing blacklists), is different from a PICS-type scenario, as PICS-compliant ratings and screening software are chosen by the user, not imposed by an ISP.

177 International harmonization of Internet standards is not unprecedented. In December, 1996, delegates from 125 countries and 90 nongovernmental organizations met in Geneva to address copyright issues on the Internet. See Nicholas W. Allard & David A. Kass, Law and Order in Cyberspace: Washington Report, 19 Hastings Comm. & Ent. L.J. 563, 590 (1997) (detailing proceedings of copyright conference); Henry V. Barry, Information Property and the Internet, 19 Hastings Comm. & Ent. L.J. 619, 631 (1997) (detailing draft treaties introduced at conference); John Schwartz, 160 Countries Set Treaty on Internet Copyrights, Wash. Post, Dec. 21, 1996, at A1 (same).

users could detect the ratings and screen out only that material that is illegal or objectionable. In this way, Germany could encourage a market in software packages that, by default, screen out materials that contain extremist propaganda or pornography. The same technology would allow American parents to configure their child's home computer to screen out indecent material, depending on what the parent deems objectionable.[178] Such a system would allow Internet regulation to occur at the most decentralized level possible in a given country, preempting the need for unilateral regulation like the COPA or the ISCA.

A. Platform for Internet Control Selection

One such system that is gaining momentum is PICS.[179] Proposed in 1996 by the World Wide Web Consortium,[180] PICS is not a ratings system, but rather a template that allows multiple independent ratings systems to be standardized and read by different screening software packages.[181] Because PICS only establishes the platform through which software can recognize an individual website's ratings, a competitive, private market can develop in *both* ratings and software. According to the World Wide Web Consortium, the PICS template "is analogous to specifying where on a package a label should appear, and in what font it should be printed, without specifying what it should say."[182] Because different countries and users wish to block

[178] Both ratings organizations and software companies have a market incentive to avoid government censorship by creating products that respond to public demand for effective screening of objectionable or illegal material. See supra notes 158-60 and accompanying text. Insofar as PICS addresses a political concern—the call for government censorship by worried constituents—the availability of easy-to-use filters that satisfy the most concerned parents may suffice as a regulatory regime vis-à-vis children. An important component of such a method is the ease of installation and use of PICS. See infra notes 209-10 and accompanying text.

[179] See Delacourt, supra note 130, at 225 (arguing for PICS); Llewellyn Joseph Gibbons, No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace, 6 Cornell J.L. & Pub. Pol'y 475, 515-17 (1997) (calling PICS and similar proposals "excellent examples of technology that permits self-help solutions in cyberspace with minimal externalities, minimal cost, and no government involvement"); Staiman, supra note 139, at 868 (describing Commission of the European Union's endorsement of PICS).

[180] The World Wide Web Consortium is a private organization of industry professionals and Internet users that opposes strict governmental regulation of the Internet.

[181] See Paul Resnick & James Miller, PICS: Internet Access Controls Without Censorship, Communications of the ACM, Oct. 1996, at 87, 87-88 (visited Mar. 15, 1999) <http://www.w3.org/pub/WWW/PICS/iacwcv2.htm> (describing and advocating for PICS, which "establishes Internet conventions for label formats and distribution methods while dictating neither a labeling vocabulary nor who should pay attention to which labels"). See generally id. (providing information and updates about PICS).

[182] Id. at 87.

different materials, PICS allows for a proliferation of ratings and screening systems which reflect diverse viewpoints and more flexible selection criteria. In allowing selective content control, PICS addresses constitutional concerns in the United States and Germany by empowering users to control content selectively while avoiding or at least limiting legislative censorship.

It is important to note up front that PICS or similar technology is not perfect. Simply stated, not all objectionable content will be screened out. Professor Goldsmith notes, however, that "indirect regulation will not be perfect in the sense of eliminating regulation evasion. But few regulations are perfect in this sense, and regulation need not be perfect in this sense to be effective."[183] Further, the adoption of such technology may not appease countries that prefer to regulate the Internet strictly through firewalls. For the vast majority of online nations, though, PICS presents a user-based alternative to legislative regulation. It can thus empower Internet users to tailor Internet content control to their own requirements and help achieve an essential goal: quelling political pressure for legislative censorship.

The PICS format has different categories of content, including sex, violence, and profanity, which may be rated in extremity from one to four.[184] Ratings can differ, but must fit into the format prescribed by the system. Web sites may be rated as a whole, based on individual pages, or simply as parts of a particular page.[185] Because PICS creates a common format for labels, any PICS-compliant selection software can process any PICS-compliant label.[186] In this way, a single website may have many labels, provided by different rating organizations, permitting neo-Nazi websites to be simultaneously unscreened in the United States while restricted in Germany. Similarly, parents can choose both their label sources and software independently, with a default baseline of unrestricted access in the United States, Germany, and in other online-friendly nations.[187]

Ratings themselves can be determined in a number of complementary ways, and ratings need not be overly widespread to achieve an acceptable level of content control. First, certain organizations could be rated benignly, such as news providers (New York Times, Weather Channel) or information services (government websites, International Monetary Fund reports). Such large-scale organizations

183 Goldsmith, supra note 167, at 1223.

184 See Resnick & Miller, supra note 181, at 90 (describing one configuration of PICS template, based on analogy to motion picture ratings).

185 See Gibbons, supra note 179, at 515.

186 See id. at 515-16 (outlining specifics of PICS proposal).

187 See id. at 516 (describing array of options for third party and self-rating services).

compose a significant portion of Internet materials and provide resources that only the most restrictive regimes would like censored. Second, content providers could self-label based on the format provided by PICS.[188] Third, a supplementary layer of government or independent organizations could rate objectionable content in countries, like Germany, with legal requirements for online control. The German government, which already has task forces dedicated to trolling the Internet,[189] could patrol for extremist propaganda, as could antipornography organizations in the United States. In this way, self-rating would be supplemented by national efforts to tailor screening software to their legal requirements.

Lastly, because ratings systems are compatible, users can rely on third parties to address some of their content concerns. As in screening software, a viable market for ratings can be established. Indeed, "anyone or any group—from Good Housekeeping magazine to the Christian Coalition—could create a ratings system, and parents could select the one that best represented their values."[190] Because many ratings systems can operate simultaneously, no single regulatory system could maintain a monopoly, allaying the concerns about over-regulation discussed above.[191]

B. Implementation of PICS

PICS is well-tailored to the legal framework of Internet regulation in the United States and Germany. By allowing parents in the United States to screen out material that they deem inappropriate for their children to see, legislative efforts to censor the Internet could be rendered moot.[192] Moreover, it would be the "least restrictive means" of content regulation available, thus meeting the *Sable* test for regula-

---

188 See Resnick & Miller, supra note 181, at 89 (calling self-labeling "a simple mechanism well-matched to the distributed nature and high volume of information creation on the Internet"). The Recreational Software Advisory Council (RSAC) provides a popular service that allows content providers to self-rate their websites. See <http://www.rsac.org/fra_content.asp> (visited Feb. 20, 1999) (stating that RSAC "empowers the public, especially parents to make informed decisions about what they and their children experience on the Internet by means of an objective, content advisory system"). Self-labeling, by itself, may be criticized. See supra Part II.C; see also Delacourt, supra note 130, at 225. See infra Part III.C for responses to these concerns in the PICS context.

189 See supra note 100 and accompanying text (noting police assigned to search Internet for illegal content).

190 Harmon, supra note 149, at D1.

191 See Roberts, supra note 171, at 118 (noting comments by Daniel Weitzner, PICS Policy Co-Chairman, that PICS would prevent single rating system from creating "monopoly foothold").

192 See supra Part I.A. (discussing political pressures for content regulation, specifically pornography).

tion of indecent material.[193] In Germany, PICS would provide the German government a method to supplement the enforcement of existing laws, rendering Internet-specific legislative censorship unnecessary.

From the user's perspective, the implementation of PICS requires installation of the screening software necessary to tailor content available on their computer or network of computers. In addition to various ratings systems, software companies can offer various packages with different levels of content screening to consumers. Thus, a competitive market in screening software could be created, lessening concerns that a universal screening system will impose subjective value judgments on users.[194] For example, a software company could have a package aimed at adults, with few (if any) filters, and one that was more restrictive that could be marketed as "family friendly."[195] Furthermore, software could be endorsed by various organizations, from the ACLU to the Freedom Foundation (or their foreign equivalents), in order to help consumers make fully informed purchase decisions.[196] Such software coincides well with the decentralized ratings systems as "[c]ompanies that prefer to remain value-neutral can offer selection software without providing any labels [and] values-oriented organizations, without writing software, can create rating services that provide labels."[197] That ratings and software packages are created by different companies and organizations further addresses the concern that one company would gain a monopoly over an Internet screening system.

---

193 See supra notes 35-38 and accompanying text (discussing *Sable*). When protecting children is the goal of a content-restrictive regulation of speech, the "least restrictive means" calculus becomes paramount in overcoming content control. According to Professor Lessig, "[W]hen kids are at stake, the only relevant question is whether there is some less burdensome way to achieve the same censoring end. If there is not, the law will stand." Lessig, supra note 1, at 631. See also Eugene Volokh, Freedom of Speech, Shielding Children, and Transcending Balancing, 1997 Sup. Ct. Rev. 141, 148 (discussing children and speech protection). Note, however, that the software companies employing the least restrictive means of technologically driven filtering would be private, not governmental, actors. This argues for a functioning market in screening software that would assure that the companies were not overregulating.

194 This is a very important point that goes to the benefits of a decentralized regulatory structure. See generally Chana R. Schoenberger, Clinton Backs Voluntary Ratings System to Let Parents Regulate Internet Use, Wall St. J., July 17, 1997, at B9 (noting that "[f]iltering software will play a major role in the administration's plan for protecting children," along with strict enforcement of existing laws, such as anti-child pornography laws).

195 Some companies already market their screening software in this fashion. See supra Part II.C.

196 For example, the Anti-Defamation League planned to distribute screening software to filter out anti-Semitic websites, and Catholic Telecom Inc. planned to develop its own rating system. See Harmon, supra note 154, at 1.

197 Resnick & Miller, supra note 181, at 88.

The implementation of screening software can occur primarily in two ways. First, software can be installed in the Internet browser itself, a configuration supported by Microsoft and Netscape.[198] This method minimizes installation problems and allows users to purchase Internet access at the same time as filtering software. Second, ISPs, independent companies, and nonprofit organizations could offer a range of software packages, at low or no cost, that would internalize the advantages of a demand-driven software market. With increased user demand, the existing market for screening software will be expanded from current NetNanny and CyberPatrol products to a wider and more refined array of screening options.[199] Organizations and online services could provide preconfigured software "for kids" or "for teenagers" in conjunction with sponsoring organizations.[200] Such software could also be marketed to users as tools to organize materials on the unruly Internet, for example, by "coolness" or newsworthiness, increasing the incentives for software companies to participate.[201]

C. *Concerns About PICS*

There are three main concerns about PICS as a system of Internet content regulation. First, some critics are concerned that PICS introduces an unregulated private censor into the medium, and that content regulation may increase rather than decrease if it is implemented.[202] By this argument, PICS would provide governments with exactly the technology that would allow for blanket censorship.[203] Instead of noting that advances in technology and increased market demand will allow for more varied and precise screening technology, some "cyberlibertarians" see PICS as a vehicle through which

198 See id. at 91. Microsoft, for example, has already incorporated an earlier version of content selection technology into its Internet Explorer web browser. See Harmon, supra note 149, at D1.

199 See supra notes 171-72 and accompanying text for a description of current screening software packages.

200 See Resnick & Miller, supra note 181, at 92 (extolling range of nonregulatory uses for PICS-compliant labels).

201 The ability of screening software to organize Internet content more generally is an important secondary benefit to the creation of ratings and software screening markets. According to Resnick and Miller, "[t]he availability of large quantities of labels will also lead to new sorting, searching, filtering, and organizing tools that help users surf the Internet more efficiently." Id. at 93.

202 See, e.g., Harmon, supra note 149, at D1 ("[A] growing number of civil libertarians argue that these technologists are in some ways acting as an unelected world government, wielding power that will shape social relations and political rights for years to come.").

203 See id. (noting critics' concern that repressive governments will use PICS to screen all dissenting political speech).

governments can control the Internet rather than as a private preemption of legislative censorship.[204]

This argument, however, neglects the decentralized nature of PICS control mechanisms.[205] Users will be aware of the materials that they are censoring off the Internet because they will choose the rater and the screening software from an array of alternatives in the market. Only when the baseline of Internet content is altered is the user not in control of content selection—for example, when Germany passes a new law to combat extremist propaganda that is applicable to the Internet. Consequently, a criticism of such governmental efforts is better directed at the government's underlying policies than at their attempt to implement them through PICS. Nazi propaganda is illegal in any medium in Germany, reflecting a policy decision borne out of historical circumstance.[206] Viewed from this perspective, PICS would not impose any new censorship, but rather enforce existing policies on the Internet.[207]

The second major concern is that PICS may not be technologically feasible due to the lack of technical acumen of parents and the computer sophistication of children. Parents may not be willing to shop around for appropriate ratings and screening packages and would prefer a governmental watchdog to do their regulating for them. Conversely, parents who do install such rating systems can be thwarted by their children, who can reroute material around the PICS labeling barriers.

While such feasibility arguments have to be addressed by any system of ratings and screening software, they do not render PICS an

---

204 See Lawrence Lessig, The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation, 5 J. Comm. L. & Pol'y 181, 184 (1997) (arguing that screening technology "will become the government's tool"). David Sobel of the Electronic Privacy Information Center provides an example of such concerns:

> This is a technique that is designed to enable one party to control what another can access. . . . The most palatable formulation of that is parent-child, but the fact is it also allows a government or an Internet service provider to take on that parental role and decide what anyone downstream is going to be able to see—and no steps have been taken to prevent that.

Harmon, supra note 149, at D1.

205 Professor Goldsmith argues forcefully that such concerns are misplaced, and that the public and the Internet industry would serve as effective checks against such a scenario. See Goldsmith, supra note 167, at 1226 ("Available technology already permits governments and private entities to regulate the design and function of hardware and software to facilitate discrimination of cyberspace information flows along a variety of dimensions, including geography, network, and content.")

206 See supra Part I.B.

207 This important distinction is highlighted by the World Wide Web Consortium, which argues that "they [are] building a tool . . . not passing a law." Harmon, supra note 149, at D1.

impotent regulatory tool. After all, one major goal of screening technology is to avoid political pressure on legislators to pass overly restrictive statutory regulation.[208] Screening technology targets those users who are concerned about Internet content and therefore are likely to lobby for such legislation, and effective screening may allay such calls. In addition, regulation need not be perfect to be effective enough to avoid legislative censorship.[209] Moreover, coordinated efforts between ISPs, software developers, and raters will quickly make PICS a system as easy to use as the Internet itself. Anyone who can install a web browser can also install screening software, and ratings choices will be made easier through the participation of sponsoring organizations.[210] Perhaps most importantly, users will have the option to leave the baseline Internet access untouched by *not* purchasing software, empowering individual users in a way that is impossible under a legislative regulatory regime. If ratings are not important to a consumer (for example, a U.S. Internet user with no children), the Internet will be available unscreened, though content that is otherwise illegal in that user's country will remain so. If a parent does not think that installing a screening mechanism is worth the effort, it is an individual balancing choice by the parent, a decision whose benefits (avoiding censorship) outweigh the costs (child's access to materials that the parent presumably has considered and accepted).

The other technological concern—that children can route around filters to get to pornography and other objectionable materials—is even less persuasive. The current problem with screening software—that its limited applicability allows easy circumvention—would be solved by the increased use of a uniform ratings template like PICS. Further, if companies adopt PICS and work for its application, such glitches can be overcome by engineers who, with market incentives to create an appealing and effective screening system, can develop methods to foolproof their products.[211]

The final major criticism of PICS is the argument that it will not be comprehensive enough to capture all offensive content, rendering it ineffective as a regulatory tool. Because PICS focuses on rating content that is posted on the World Wide Web, it misses other forms

---

208 See supra Part III.A.

209 See supra note 183 and accompanying text (noting that few regulatory schemes capture all violators, but that imperfection does not gut such regulation).

210 See supra notes 190-91 (noting that users can select ratings through reference to sponsoring organizations).

211 See Goldsmith, supra note 167, at 1224-30 (belittling concerns that engineers cannot construct sufficiently inclusive screening system). In addition, software developers would be well advised to take on some pint-sized informal consultants if it would facilitate security of screening mechanisms from children.

of electronic communication such as e-mail. Such concerns are real but misplaced. The driving force for content regulation has been publicly disseminated words and images, not private communications between individuals or groups. Websites provide deviant Internet users a unique ability to spread their racist hate or pornographic images to large groups of individuals. E-mail is a method of communication that is akin to "snail mail,"[212] or regular postal delivery. Privacy concerns are involved with e-mail, further complicating any screening regime based on individual communications.[213] In sum, PICS addresses the vast majority of concerns about content control on the Internet by focusing on the World Wide Web.

It appears that the U.S. government would support a PICS-like proposal. The Interagency Working Group on Electronic Commerce, a presidentially appointed group composed of officials ranging from the National Security Council to the Federal Trade Commission, issued a conclusive report supporting a nonregulatory, free-market approach to Internet technology.[214] The Group offered a global regulatory approach that (1) fosters the Internet as a minimally regulated, market-driven environment, (2) ensures a "transparent" and harmonized global legal environment, and (3) allows "competition and consumer choice" to shape the marketplace.[215] Furthermore, the Group emphasized that "[t]he U.S. government supports the broadest possible free flow of information across international borders"[216] and urged that any content controls should come from self-regulation, ratings systems, and technological solutions.[217] Joint government and Internet industry conferences designed to promote nonlegislative solutions to Internet regulation followed this initiative.[218]

---

212 That is, mail carried by national postal services.

213 See, e.g., Scott A. Sundstrom, Note, You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring, 73 N.Y.U. L. Rev. 2064, 2067-68 (1998) (introducing privacy issues related to e-mail monitoring).

214 See Interagency Working Group on Electronic Commerce, Framework for Global Electronic Commerce (1997) (visited Mar. 15, 1999) <http://www.whitehouse.gov/WH/New/Commerce/about.html> (reporting findings of Internet working group).

215 Id.

216 Id.

217 See id. (discussing content-related market access issues).

218 See Munro, supra note 159, at 404, 405-07, 409 (outlining joint government-industry initiatives). President Clinton has specifically indicated a desire to couple an unregulated free-trade zone on the Internet with measures to "make the Internet safe for children." The White House: Remarks by the President in Announcement of Electronic Commerce Initiative, M2 Presswire, July 2, 1997, available in 1997 WL 11937386. To do so, he proposed a PICS-like standardized rating system:

> [I]t is especially important . . . to give parents and teachers the tools they need to make the Internet safe for children. A hands-off approach to electronic commerce does not mean indifference when it comes to raising and protecting

Additionally, prospects for a PICS-type solution are good in Germany and the European Union (EU). The EU has recommended an Internet policy that would internalize countries' differences into a regulatory framework by decentralizing decisions about what content to regulate while creating a uniform structure of regulation.[219] Specifically, the European Parliament stated, "What is considered to be harmful [on the Internet] depends on cultural differences. . . . Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible."[220]

CONCLUSION

Domestic policy goals and legal constraints on Internet regulation will differ in each country, as illustrated by the differences between the United States and Germany. A viable regulatory regime must internalize these differences and allow enforcement of domestic political goals on the Internet. The United States and Germany, countries with similar approaches to free speech, differ on what content they wish to control on the Internet, indicating the wide disparity of policy choices that an international Internet regulatory structure must accommodate. However, as this Note has argued, existing systems of regulation that ban certain content from the Internet altogether overregulate speech and risk stifling the growth of Internet technology. The adoption of a standardized ratings template, alongside a competitive market in ratings and screening software, will best allow the United States, Ger-

---

children. I ask the industry leaders here today to join with us in developing a solution for the Internet that will be as powerful for the computer as the V-Chip will be for television, to protect children in ways that are consistent with the First Amendment.

Id.

219 See Council Moves to Restrict Illegal Content on the Internet, European Report, Nov. 30, 1996, available in 1996 WL 11074437. These proposals were the result of increased calls to prevent traffic in criminal and offensive material. See EU Ministers Order Study About Regulating Internet, Wall St. J., May 3, 1996, at A7 (noting calls for Internet content control in Europe). The EU formalized these policies in a November 1996 resolution that called on member states to take measures to promote regulatory regimes administered by third parties representing providers and users of Internet services. The EU further recommended the development of effective codes of conduct along with rating and filtering mechanisms. See Council Moves to Restrict Illegal Content on the Internet, supra (noting that resolution specifically mentioned PICS in its discussion of filtering systems). This policy was echoed in the 1997 "Bonn Declaration," in which European governments agreed to keep a largely hands-off approach to regulating the Internet, leaving it up to industry and international accord to police content. See European Officials Agree with U.S. on Internet Self-Regulation, Associated Press, July 8, 1997, available in 1997 WL 4874072 (detailing meeting of government officials and Internet specialists leading to Bonn Declaration).

220 Testing the Boundaries, supra note 132, at D1.

many, and other online countries to balance enforcement of domestic policy goals with protection of free speech. Such a regime can help decentralize regulation, empower users to make their own choices about content, and, perhaps most importantly, avoid more drastic attempts by governments to impose content control through censorship.