

## RENO V. ACLU

By David K. Djavaherian

Increasingly, the American legal system's ability to adapt to technological changes is strained the dynamic nature of technology. When faced with rapid development, lawmakers find themselves struggling to keep up with the pace of innovation. In the ambit of this struggle, *Reno v. ACLU*,<sup>1</sup> which marks the United States Supreme Court's first brush with regulation of the Internet, should be considered a legal milestone. In *Reno*, the Court was called upon to apply the First Amendment to this new medium of communications—to decide how much leeway the government has in regulating on-line content. The case pitted an amalgam of free speech activists against the Communications Decency Act of 1996 (CDA).<sup>2</sup> Even before the CDA became law, it was widely suspected that it would be struck down on First Amendment grounds if enacted.<sup>3</sup> The Court in *Reno* confirmed these suspicions by holding the CDA unconstitutional.<sup>4</sup> In the process, the Court issued an important statement on the Internet as a medium of communications: expressive content on the Internet is entitled to the full protection of the First Amendment—the same degree of protection as that afforded to print. But this mandate gives little indication as to how to solve the problem that led to enactment of the CDA: protecting children from on-line smut. Thus, in addition to examining and explaining the Court's First Amendment argument, this comment discusses the various methods of Internet content regulation that are presently available.

### I. LEGISLATIVE BACKGROUND

Senator James Exon (D-Neb.) introduced the CDA on February 1, 1995.<sup>5</sup> Senator Exon drummed up support for the CDA by passing around

---

© 1998 Berkeley Technology Law Journal & Berkeley Center for Law and Technology.

1. \_\_\_ U.S. \_\_\_, 117 S. Ct. 2329 (1997).

2. 47 U.S.C.A. § 223 (West Supp. 1997).

3. See, e.g., Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 67 (1996) (quoting Speaker of the House Newt Gingrich, who argued that the CDA "is clearly a violation of free speech .... I don't think it is a serious way to discuss a serious issue, which is, how do you maintain the right of free speech for adults while also protecting children in a medium which is available to both?").

4. *Reno*, 117 S. Ct. at 2351.

5. See Cannon, *supra* note 3, at 52, 57.

his "Blue Book," a collection of pornography gathered from the Internet.<sup>6</sup> Despite some early resistance,<sup>7</sup> the Act was included in the Senate's version of the telecommunications bill.<sup>8</sup> However, the Act encountered stronger opposition in the House.<sup>9</sup> The House passed the Online Family Empowerment Amendment, which "proclaimed an Internet free of government interference," but included no method of enforcing its claims, and exempted the CDA from its purview.<sup>10</sup> However, in a joint conference committee replete with CDA supporters,<sup>11</sup> the CDA and the Online Family Empowerment Amendment (both with a few minor adjustments) were together incorporated into the final version of the Telecommunications Act.<sup>12</sup> Despite the previous opposition to the CDA in the House, the Telecommunications Act of 1996, which incorporated the CDA, became law on February 8, 1996.<sup>13</sup> That same day, the ACLU and nineteen other plaintiffs filed suit against the Attorney General, challenging the constitutionality of the CDA's provisions.<sup>14</sup>

---

6. See Cannon, *supra* note 3, at 64. The Blue Book "is theorized to have helped reluctant senators vote for the CDA. No senator wanted to make what could be construed as a pro-pornography vote." *Id.* at 64.

7. Senator Leahy introduced a competing amendment which proposed the federal government take no additional efforts to regulate the Internet, and accused the CDA of catering to individuals phobic of on-line pornography. See Cannon, *supra* note 3, at 65-66.

8. See Cannon, *supra* note 3, at 71 (citing 141 CONG. REC. S8386-87, S8347 (daily ed. June 14, 1995)).

9. See *Reno*, 117 S. Ct. at 2338 n.24 (discussing opposition in House). It is suggested that the House was more resistant to Internet regulation because of its generally younger and more Internet-savvy composition. See Cannon, *supra* note 3, at 67.

10. Cannon, *supra* note 3, at 67-69 (criticizing the act as "a bill without a verb" and noting it "specifically and curiously stated that '[n]othing in this section shall be construed to impair the enforcement of section 223 of Title 47,' the very statute the CDA sought to amend.")

11. Senators Exon and Gordon, co-sponsors of the CDA, were named to the Telecommunications conference committee, and all of the other senators on the committee had voted for the CDA. The lone opponent of the CDA on the committee was Rep. White, who co-sponsored the Online Family Empowerment Amendment. See *id.* at 91.

12. See *id.* at 92.

13. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C., 15 U.S.C. §§ 18, 5714, and § 18 U.S.C. §§ 1462, 1465, 2422). The Telecommunications Act consists of seven titles, outlining a broad array of regulatory and deregulatory policies for a number of media. The CDA is codified in Title V. The full effect of the Telecommunications Act on previous United States Code sections, as well as the range of the CDA, is listed in 47 U.S.C.A. § 609 (West Supp. 1997).

14. *ACLU v. Reno*, 929 F. Supp. 824, 826 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997).

Two provisions of the CDA were challenged in *Reno*. Section 223(a)(1)(b) (the “indecent transmission” provision) prohibits the creation or solicitation, and initiation of “indecent or obscene” transmissions, “knowing that the recipient is under 18 years of age.”<sup>15</sup> Violating this provision required actual knowledge that the recipient was a minor. Section 223(d)(1) (the “patently offensive display” provision) prohibits the knowing sending or displaying of messages, “in a manner that is available to persons under 18 years of age,” which depict or describe “sexual or excretory activity or organs” in a way that is “patently offensive” in the context of “contemporary community standards.”<sup>16</sup> Unlike the indecent transmission provision, violation of the patently offensive display provision would occur even if the speech was not actually directed at youths, so long as the defendant knew that the communication would be available to minors.

Violation of the CDA is punishable by criminal fines and up to two years imprisonment.<sup>17</sup> However, two affirmative defenses limit the application of these provisions. “Good faith, reasonable, effective, and appropriate actions” to prevent access by minors to otherwise actionable communications,<sup>18</sup> or use of specified screening methods such as requiring adult access codes or credit card numbers,<sup>19</sup> prevent prosecution under both the indecent transmission and patently offensive display provisions.

## II. CASE SUMMARY

### A. Doctrinal Background

The plaintiffs argued that the CDA was facially invalid because it was both “vague” and “overbroad.” Vague laws violate the Fifth Amendment’s due process standards.<sup>20</sup> Though absolute clarity of law is unattainable given its linguistic nature, procedural due process mandates that statutory commands be drawn with clarity sufficient to (1) provide citizens

---

15. 47 U.S.C.A. § 223(a)(1)(b) (West Supp. 1997).

16. *Id.* § 223(d)(1).

17. *Id.* § 223 (a), (d).

18. *Id.* § 223(e)(5)(a).

19. *Id.* § 223(e)(5)(b).

20. “No person shall ... be deprived of life, liberty, or property, without due process of law.” U.S. CONST. amend. V.

with notice of the commands of the law,<sup>21</sup> and (2) prevent excessive discretion in the enforcement of the law.<sup>22</sup>

Overbroad laws violate the First Amendment.<sup>23</sup> Unless the First Amendment is implicated, a facial challenge to a statute will not succeed unless the challenger can prove that the statute has no constitutionally acceptable applications.<sup>24</sup> However, pursuant to overbreadth doctrine, a statute is subject to facial invalidation if (1) it burdens protected expression; (2) it lacks narrow tailoring—that is, if the burden on expression is overbroad in relation to the statute’s “plainly legitimate sweep,” and (3) no narrowing construction is available.<sup>25</sup>

## B. The District Court’s Decision

Pursuant to a statutorily mandated procedure for judicial review, the challenge to the CDA led to creation of a novel judicial panel. Though a single judge initially handled the suit, a facial challenge brought against the CDA sparked the formation of a three-judge panel to hold the trial.<sup>26</sup>

When the ACLU and the other plaintiffs first filed suit in the Eastern District of Pennsylvania, District Court Judge Buckwalter was assigned to

---

21. See *Connally v. General Const. Co.*, 269 U.S. 385, 391 (1926) (a law couched “in terms so vague that men of common intelligence must necessarily guess at its meaning” violates due process).

22. See *Kolender v. Lawson*, 461 U.S. 352, 358 (1983) (vague criminal statutes threaten due process by enabling “policemen, prosecutors, and juries to pursue their personal predilections”).

23. Congress shall make no laws ... abridging the freedom of speech.” U.S. CONST. amend I. “Speech” is interpreted broadly to encompass many forms of “expression.” See, e.g., *United States ex rel. Milwaukee Social Democratic Publ’g Co. v. Burleson*, 255 U.S. 407, 431 (1921) (Brandeis, J., dissenting) (first articulating the speech-as-expression interpretation).

24. See *United States v. Salerno*, 481 U.S. 739, 745 (1987) (regulations not implicating the First Amendment are facially invalid only if there is no set of circumstances under which the law would be valid). But see Michael C. Dorf, *Facial Challenges to State and Federal Statutes*, 46 STAN. L. REV. 235, 236 (1994) (“[T]he *Salerno* ‘no set of circumstances’ principle does not accurately characterize the standard for deciding facial challenges.”).

25. See *Broadrick v. Oklahoma*, 413 U.S. 601, 615-16 (1973); see generally Richard H. Fallon, *Making Sense of Overbreadth*, 100 YALE L.J. 850, 863 (1991).

26. Notwithstanding any other provision of law, any civil action challenging the constitutionality, on its face, of this title, or any provision thereof, shall be heard by a district court of 3 judges convened pursuant to the provisions of section 2284 of title 28, United States Code.” Telecommunications Act of 1996, Pub. L. No. 104-104, § 561(a), 110 Stat. 56, 142-43 (codified as a note to 47 U.S.C. § 223). The referenced section provides that “A single judge may conduct all proceedings except the trial.” 28 U.S.C. § 2284(b)(3) (1994).

the case. Finding the statute's indecency provision unconstitutionally vague, he issued a temporary restraining order against enforcement of the CDA soon after the case was filed.<sup>27</sup> The three-judge panel was then convened for trial; it consisted of Judge Buckwalter, District Judge Dalzell, and Chief Judge Sloviter of the Court of Appeals for the Third Circuit.<sup>28</sup>

The panel unanimously granted a preliminary injunction against enforcement of the CDA.<sup>29</sup> Together, the panel made extensive factual findings,<sup>30</sup> but each judge on the panel wrote a separate opinion. Judge Buckwalter and Chief Judge Sloviter found the CDA unconstitutionally overbroad under the First Amendment and unconstitutionally vague under the Fifth Amendment.<sup>31</sup> Judge Dalzell found the CDA overbroad but not vague.<sup>32</sup> His opinion extols the speech-enhancing and democratic character of the Internet, and concludes that "any regulation of protected speech on this new medium [would be unconstitutional]."<sup>33</sup>

### C. The Supreme Court Meets the Internet

Pursuant to "fast-track" review provisions applicable to the CDA,<sup>34</sup> the government directly appealed the district panel's decision to the Supreme Court. The Court unanimously held the CDA unconstitutional as overbroad.<sup>35</sup> It did not, however, reach the question of the CDA's vagueness, except indirectly, as a factor to be considered in determining the CDA's overbreadth.<sup>36</sup>

---

27. *ACLU v. Reno*, 929 F. Supp. 824, 826 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997).

28. *See id.* at 826-27.

29. *See id.* at 849 ("[P]laintiffs have shown irreparable injury, no party has any interest in enforcement of an unconstitutional law, and therefore the public interest will be served by granting this preliminary injunction.").

30. *See id.* at 830-49. The court's findings related to the nature of the Internet, Internet content, and the viability of various types of filtering software. The Supreme Court relied on many of the trial court's factual assertions. *See Reno v. ACLU*, \_\_\_ U.S. \_\_\_, 117 S. Ct. 2329, 2334-37 (1997).

31. *ACLU*, 929 F. Supp. at 858-59 (Judge Buckwalter), 857 (Judge Sloviter).

32. *See id.* at 867-69, 883.

33. *Id.* at 867.

34. "Notwithstanding any other provision of law, an interlocutory or final judgment, decree, or order of the court of 3 judges . . . holding this title or an amendment made by this title, or any provision thereof, unconstitutional shall be reviewable as a matter of right by direct appeal to the Supreme Court." Telecommunications Act of 1996, Pub. L. No. 104-104, § 561(b), 110 Stat. 56, 143 (codified as a note to 47 U.S.C. § 223).

35. Six justices joined Justice Stevens's opinion. Justice O'Connor, joined by Chief Justice Rehnquist, filed a concurrence holding the CDA unconstitutional on somewhat narrower grounds than the majority.

36. *See Reno*, 117 S. Ct. at 2343-45.

Discussion of the case will proceed in three parts, paralleling the three criteria for overbreadth. Part II.C.1. will consider whether the CDA burdens speech protected by the First Amendment, and if so, whether full First Amendment protection is justified. Part II.C.2. will discuss the burden imposed by the CDA in relation to the government interest it serves. Part II.C.3. will examine the possibility of judicially narrowing the scope of the CDA.

### 1. *The CDA Regulates Protected Expression*

It is well established that obscene expression is not protected under the First Amendment.<sup>37</sup> Thus the plaintiffs in *Reno* did not challenge the CDA provisions regulating on-line obscenity.<sup>38</sup> But not all sexually explicit material is obscene, and the CDA's regulation of "indecent" and "patently offensive"<sup>39</sup> material burden expression protected by the First Amendment.

However, the government did have a compelling interest in enacting the CDA: protecting minors from "indecent" and "patently offensive" expression.<sup>40</sup> Even though such speech is protected by the First Amendment when adults are involved, the scope of minors' First Amendment rights is less extensive.<sup>41</sup>

Moreover, speech harmful to minors can be regulated more stringently in some media than it can be in others.<sup>42</sup> Over the past thirty years, the Supreme Court has fashioned a "medium-specific" approach to content

---

37. See, e.g., *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571-72 (1942). Obscenity is defined under a three-part test, all parts of which must be met: (1) The average person, applying contemporary community standards, would find the work, taken as a whole, appeals to the prurient interest; (2) the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law; and (3) the work, taken as a whole, lacks serious literary artistic, political, or scientific value. See *Miller v. California*, 413 U.S. 15, 24 (1973). Under this definition, only depictions or descriptions of "hard core" sexual conduct are obscene. See *id.* at 27-28.

38. See *Reno*, 117 S. Ct. at 2349. Obscenity is oft regulated in other contexts. See, e.g., 18 U.S.C. § 1465 (1994) (prohibiting transportation in commerce of obscene material); *id.* § 1466 (1994) (prohibiting engaging in the business of selling obscene materials).

39. It is true that the "patently offensive" language in the CDA incorporates some of the language of the *Miller* test for obscenity, see *supra* note 37, but, as the Court points out, incorporating one element of the three-pronged *Miller* test is not sufficient. See *Reno*, 117 S. Ct. at 2345.

40. See *Ginsberg v. New York*, 390 U.S. 629, 638-39 (1968) (establishing government interest in protecting minors from sexually indecent speech).

41. See, e.g., *id.* at 639-40.

42. For a discussion of the rationale which led the Court to tailor First Amendment protection to the media involved, see *infra* part IV(A).

regulation. Print has always received the full quantum of First Amendment protection.<sup>43</sup> But in an approach that began with *Red Lion Broadcasting Co. v. FCC*<sup>44</sup> and was refined in *FCC v. Pacifica Foundation*,<sup>45</sup> the Court found that broadcasting's history of governmental regulation, the scarcity of bandwidths available, and the intrusive nature of the medium justify affording a lesser degree of First Amendment protection to broadcast expression.<sup>46</sup> More recently, the Court extended this medium-specific approach to find content on cable television more constitutionally protected than broadcasting, but nevertheless not so constitutionally insulated as printed content.<sup>47</sup> Because the Internet has no history of lesser protection,<sup>48</sup> no comparable bandwidth limitations, and because accessing indecent expression on the Internet usually requires a "series of affirmative steps,"<sup>49</sup> the Court held the Internet, as a medium, most analogous to print, and therefore deserving of the strongest First Amendment protection.<sup>50</sup>

## 2. *The CDA's Regulation of Protected Expression is Overbroad*

The Court found that a number of factors contributed to making the CDA an overbroad law subject to facial invalidation.<sup>51</sup> Specifically, one problem with the CDA was that it was somewhat vague.<sup>52</sup> Congress' failure to define the standards by which "indecent" or "patently offensive" material would be adjudged, and confusion between the two standards Congress used to regulate communications left the Court weary of the "chilling effect" that the CDA's commands may have on the exercise of free speech.<sup>53</sup> The resulting uncertainty in applying the CDA "undermines the likelihood that the CDA has been carefully tailored to the congres-

43. See, e.g., *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241, 258 (1974).

44. 395 U.S. 367 (1969).

45. 438 U.S. 726 (1978).

46. See *id.* at 741 n.17 (1978) ("[I]t is well settled that the First Amendment has a special meaning in the broadcasting context.").

47. See *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 637-662 (1994).

48. *Reno v. ACLU*, \_\_\_ U.S. \_\_\_, 117 S. Ct. 2329, 2342 (1997).

49. *Id.*

50. *Id.* at 2343-44. This finding, and its ramifications, will be discussed further *infra* part III(A).

51. This multi-faceted approach, common in First Amendment jurisprudence, has led some scholars to decry First Amendment doctrine as "infinitely complex." See, e.g. Fallon, *supra* note 25, at 864. It has led others to describe the doctrine as effectively a balancing methodology. See, e.g., S. SHIFFRIN, *THE FIRST AMENDMENT, DEMOCRACY, AND ROMANCE* 9-45 (1990), J. ELY, *DEMOCRACY AND DISTRUST* 105-16 (1980) (criticizing the balancing approach).

52. The Court, however, did not reach the question as to whether the CDA was so vague as to violate the Fifth Amendment.

53. *Reno*, 117 S. Ct. at 2344.

sional goal of protecting minors from potentially harmful materials.”<sup>54</sup> In other words, the CDA’s vagueness contributes to its overbreadth. The Court, however, avoids quantifying the ramifications of its finding.

Next, the Court begins a more formal analysis of the CDA’s overbreadth. The problem confronted was that the CDA’s regulations, though aimed at protecting children, would have the effect of limiting adults’ access to speech that they have a constitutional right to receive. Because the Court found that the CDA’s mandates were “content-specific”—that is, they were aimed specifically at the content of the regulated expression, rather than at its “secondary effects”<sup>55</sup>—the CDA would be overbroad unless “narrowly tailored” to achieve the compelling governmental interest of protecting minors from harmful speech on the Internet.<sup>56</sup> Moreover, given the CDA’s vague character and the full protection afforded the Internet as a medium, it is especially important that the means not outpace the ends; the government may not “reduc[e] the adult population ... to ... only what is fit for children.”<sup>57</sup> The Court invoked its strictest standard of scrutiny, concluding:

In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if *less restrictive alternatives* would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.<sup>58</sup>

Alternative methods of Internet content regulation, such as “tagging” and filtering software, were then considered.<sup>59</sup> Because the Court determined that the government failed to prove that such methods would not be as ef-

---

54. *Id.*

55. *Id.* at 2342 (distinguishing *Renton v. Playtime Theaters*, 475 U.S. 41 (1986)). *But see Reno*, 117 S. Ct. at 2351-57 (O’Connor, J., concurring and dissenting) (analyzing the CDA as a form of “cyberzoning” with the purpose of establishing “adult zones” on the Internet, rather than of regulating content). Regulations aimed at the “secondary effects” of expression (“content-neutral” regulations) are subject to a lesser degree of judicial scrutiny than “content specific” regulations; content-neutral regulations are constitutional if they serve a substantial governmental interest, and do not unreasonably limit alternative channels of communication. *See, e.g., Renton*, 475 U.S. at 47; *Clark v. Community for Creative Non-Violence*, 468 U.S. 288, 293 (1984).

56. *See Broadrick v. Oklahoma*, 413 U.S. 601, 615-16 (1973).

57. *Reno*, 117 S. Ct. at 2346 (quoting *Denver Area Ed. Telecommunications Consortium, Inc. v. FCC*, 116 S. Ct. 2374, 2393 (1996)).

58. *Reno*, 117 S. Ct. at 2346 (emphasis added).

59. For a discussion of such technologies, see *infra* part III(B).

fective as the CDA at protecting minors from indecent and patently offensive expression on the Internet, the CDA was held overbroad.<sup>60</sup>

### 3. *Only a Trivial Narrowing Construction is Available*

The government, as an argument of last resort, asked the Court to use the CDA's severability clause<sup>61</sup> to remove its overbroad elements, and to construe non-severable terms as narrowly as possible.<sup>62</sup> The Court essentially refused to do so, arguing that it is beyond the Court's province to do the sort of substantive revision that would be required in order to salvage a material portion of the CDA.<sup>63</sup> Instead the "patently offensive display" and "indecent transmission" provisions were found facially invalid. With these provisions struck, only the CDA's regulation of obscenity, which, as noted above, receives no protection under the First Amendment, was upheld.<sup>64</sup>

## III. DISCUSSION

### A. The Medium-Specific Scrutiny Approach as Applied to the Internet

The Court's opinion in *Reno v. ACLU* begins with the proposition that the Internet is entitled to the most stringent degree of protection available under the First Amendment. Justification for heightened regulation of other mediums has been threefold: (1) historical regulation; (2) scarcity of access;<sup>65</sup> and (3) the "captive audience" or "invasive nature" problem.<sup>66</sup>

The historical argument is weak both theoretically and as applied to the Internet. Theoretically, it is unclear why past governmental regulation

---

60. *Reno*, 117 S. Ct. at 2347. *But see infra* part III(B) (discussing availability of alternatives to the CDA); Eugene Volokh, "Freedom of Speech, Shielding Children, and Transcending Balancing," 1997 SUP. CT. REV. (forthcoming 1998) (arguing that the alternatives considered by the Court are not presently available or effective, and so, factually, no "less restrictive alternatives" to the CDA are available).

61. "If any provision of this chapter or the application thereof to any person or circumstances is held invalid, the remainder of the chapter and the application of such provision to other persons or circumstances shall not be affected thereby." 47 U.S.C. § 608 (1994)

62. *See Reno*, 117 S. Ct. at 2350.

63. *See id.*

64. *See id.*

65. That is, in the broadcast context, there are a limited number of available frequencies (channels) from which "speakers" can communicate, so permitting indecent speech would necessarily come at the expense of other types of expression. *See Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 388 (1969).

66. *See Reno*, 117 S. Ct. at 2343.

of a medium should serve as a justification for infringing on constitutional rights. And practically, the Internet, as a relatively new medium, has no history of significant governmental regulation.<sup>67</sup> Likewise, the access argument is inapplicable to on-line communications because bandwidth limitations comparable to those that affect broadcasting are not present.<sup>68</sup>

Applying the third argument to the Internet is more complicated. Relying on the trial Court's findings of fact, the Court finds that content on the Internet is seldom encountered by accident.<sup>69</sup> However, seemingly innocuous net-searches such as "teen," "eagle," or "candy" may lead users directly and unwittingly to sexually explicit web sites.<sup>70</sup> Moreover, mass e-mail advertisements or "spam" often contain a variety of pornographic solicitations.<sup>71</sup> Though the Court correctly finds that the Internet is not as invasive as broadcasting,<sup>72</sup> it overestimates a user's ability to control the content that is received.

Nevertheless, the Court is satisfied with its finding that broadcasting is a more "invasive" medium than the Internet, and extends full First Amendment protection to the Internet. This will have three ramifications. First, as attested to by the failure of the CDA, it will be more difficult to enact Internet content-regulations. Governmental regulations will have to

---

67. See *id.* at 2344. It is true, however, that the Internet is the child of ARPANET, which was funded by the government. See *ACLU v. Reno*, 959 F. Supp. 824, 831-32 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997). Thus some sort of ownership justification may seem plausible. However, a variety of considerations make such a theory of very limited weight. First, the Internet has been free from government control for a number of years, and has been operating without material governmental interference during that time. Thus, even if the government was initially entitled to control its content, the right to do so may have been abandoned or adversely possessed. Second, the prevalence and value of the Internet is not attributable to the government, but rather to the private users that have made it widespread. Cf. *Lotus Devel. Corp. v. Borland Intl., Inc.*, 49 F.3d 807, 821 (1st Cir. 1995) (Boudin, J., concurring) ("[I]t is hard to see why customers who have learned the Lotus menu and devised macros for it should remain captive of Lotus because of an investment in learning made by the users and not by Lotus."). Third, First Amendment protections are not trumped by governmental assertions of property rights when the property is a "public forum." See *Perry Education Assn. v. Perry Local Educators' Assn.*, 460 U.S. 37, 45-46 (1983); David J. Goldstone, *A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech*, 69 U. COLO. L. REV. 1, 7-10 (1998) (discussing application of public forum doctrine to Internet).

68. See *Reno*, 117 S. Ct. at 2343.

69. See *id.* at 2343 (citing *ACLU*, 929 F. Supp. at 844).

70. See, e.g., Brad Stone, *Coping With the Internet*, NEWSWEEK EXTRA, Winter 1997, at 15 ("type in the word 'teen' and sex sites are mixed in with your results").

71. See *id.* at 20.

72. See *Reno*, 117 S. Ct. at 2343.

survive strict scrutiny, and so the power of Congress and the states to regulate the Internet will be more constrained in the future.

Second, this difficulty will spur the development and use of filtering technologies and other private means of shielding unwanted content.<sup>73</sup> Parents, schools, and even libraries<sup>74</sup> are already hurrying to find and implement effective means of content regulation.<sup>75</sup> The more stringently the Internet is protected from public regulation, the more important these private measures will become in regulating content.

Third, the Court's medium-tailored analysis of the First Amendment will become much less significant. As the Internet grows, it is continually incorporating other media, such as television, and as it comes to offer a viable alternative to broadcasting and cable, those industries will begin televising their programs over the Internet. Programs on "Internet TV," unlike those carried on traditional mediums, will be fully protected by the First Amendment, and there will be little content transmitted via broadcast or cable that is not also on the Internet.<sup>76</sup> Thus, eventually, it is unlikely that a significant portion of expression will be burdened with the lesser degree of First Amendment protection afforded to broadcast and cable.

## B. Regulating Internet Content After *Reno v. ACLU*:

As noted above, the full protection afforded the Internet as a medium will spur the development of private means of protecting minors from harmful content.<sup>77</sup> There are currently three general methods of doing so,

---

73. See *infra* part III(B).

74. There have been a number of controversies involving libraries and the adoption of filtering technologies. Libraries have been attacked from both sides: Those libraries that have introduced filtering software have been criticized by free speech activists for discouraging the exchange of ideas. Those that have not have been hounded by activists who claim that the librarians are distributing pornography of minors. See Jim Rendon, *No Place is Safe*, WIRED, Dec. 1997, at 102. The American Library Association has criticized filtering software as imprecise and arbitrary. See *id.*

75. See, e.g., Glenn Kubota, *Public School Use of Internet Filtering Software: Book Banning Reincarnated?*, 17 LOYOLA L.A. ENT. L.J. 687, 687-89 and accompanying notes (1997) (many school districts already use some form of filtering software).

76. Cf. *Denver Area Educational Telecommunications Consortium v. FCC*, \_\_\_ U.S. \_\_\_, 116 S. Ct. 2374, 2402 (1996) (Souter, J., concurring) ("[W]e have to accept the likelihood that the media of communication will become less categorical and more protean.")

77. See *supra* part III(A). Cf. Jane Black, "Lewd and Rude: Blocking the Bad Without Booting the Good," NEWSWEEKEXTRA, Winter 1997, at 21 ("In Cyberspace, where anarchy rules and even a typo can lead to a pornography site, parents need help in constructing kid-safe zones."). A number of technology and media companies have recently embarked on a public relations campaign design to educate parents to install filtering products on their computers. See Rajiv Chandrasekaran, *Internet Firms to Kid-Proof Sex Sites*, S.F. CHRON, Dec. 1, 1997, at A1.

each of which will be considered in turn: (1) coercion, or what has been termed "low-tech" regulation;<sup>78</sup> (2) verification of age and/or identity; and (3) a variety of forms of "filtering" software. A discussion of their attributes and shortcomings helps demonstrate that none of the three methods is as effective as the CDA would have been at shielding minors from harmful on-line content. If this is so, then there are no less restrictive alternatives *at least as effective* as the CDA, and the Court's finding to the contrary<sup>79</sup> is in error.

### 1. "Low-Tech" Regulation

The simplest form of regulation is coercion. While coercive legislation such as the CDA is constrained by the *Reno* opinion, parents, schools, and other Internet access providers can use coercive measures to regulate the content that is actually accessed on their computers. Parents, for example, can formulate "house rules" for their children's Internet use, and establish consequences for breaking those rules.<sup>80</sup>

Such a method may be feasible on a grander scale. For example, the Los Angeles Unified School District recently established an "Acceptable Use Policy" that students and parents must sign prior to the students' receiving Internet access.<sup>81</sup> The policy establishes rules against intentionally accessing pornographic materials, and violations are punished by the cancellation of access privileges.<sup>82</sup> The key to regulatory authority here is not only the fact that all users are minors, but also that access is considered a "privilege," and so students cannot refuse to be constrained by the terms of the use agreement.

However, as with all coercive measures, "low-tech" regulation can only be as effective as its enforcement mechanism. Monitoring the usage habits of minors is probably impractical, and minors might still access indecent materials on unmonitored computers (for example, at friends' houses). These problems leave "low-tech" efforts to regulate on-line content in need of an effective supplement.

### 2. Verification Methods

Another method of restricting minors' access to harmful on-line materials is to require that some method of age verification be used at sites that

---

78. Kubota, *supra* note 75, at 695.

79. See *Reno v. ACLU*, \_\_\_ U.S. \_\_\_, 117 S. Ct. 2329, 2347 (1997); see also *supra* part II(C)(2).

80. See Stone, *supra* note 70, at 20.

81. See Kubota, *supra* note 75, at 695-96.

82. See *id.* at 696.

contain indecent expression, such as the use of credit cards or of a personal identification password. The district court considered such a requirement, but found that current methods of verification are too expensive, and would thus impose an unfair burden on non-commercial content providers.<sup>83</sup> Furthermore, requiring credit card verification would restrict the access of adults that do not have credit cards,<sup>84</sup> and requiring credit cards or personal identification numbers might restrict the access of adults concerned with their privacy.<sup>85</sup> And, as the Supreme Court noted, there is little "evidence that these verification techniques actually preclude minors from posing as adults."<sup>86</sup> This array of problems makes a verification-based methodology for controlling Internet content of limited usefulness.

Nevertheless, legislation has recently been proposed which would institute a mandatory regime of verification for all commercial providers of materials "harmful to minors."<sup>87</sup> Currently, most commercial sites require a credit card, but the proposed legislation would also require use of a verification method before display of the "teaser" images commonly found in the publicly accessible areas of commercial sites.<sup>88</sup> Critics argue that the bill is vague because it fails to define its "harmful to minors" standard, and also unfair because it burdens commercial sites without restricting the provision of "harmful" materials at free sites.<sup>89</sup> Given these problems and those discussed above, such a legislatively mandated system of verification should fail to pass *Reno's* constitutional test.

### 3. Filtering Software

Generally, filtering software is designed to limit a user's access to Internet sites that contain sexually explicit content, and it is currently the most promising method of Internet content regulation.<sup>90</sup> Such software is commercially available from a number of companies, and most will soon include compatibility with the Platform for Internet Content Selection

---

83. See *ACLU v. Reno*, 929 F. Supp. 824, 846 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997).

84. See *id.*

85. See *id.* at 847.

86. *Reno*, 117 S. Ct. at 2349; see also *ACLU*, 929 F. Supp. at 847.

87. See Jon Schwartz, *Another Bid to Ban Web Porn*, S.F. CHRON., Nov. 14, 1997 at B1 (discussing "Son of CDA" legislation introduced by Senator Dan Coates).

88. See *id.* at B1.

89. See *id.* at B2.

90. See, e.g., Chandrasekaran, *supra* note 77, at A11; Andrew L. Shapiro, *Letter from Aspen: Blocking Software Triggers a Rocky Mountain High*, WIRED, Nov. 1997, at 118 (quoting Ralph Reed, head of the Christian Coalition, stating "[t]he wave of the future is going to be filtering software.").

(PICS), a rating system that is rapidly developing on the Internet.<sup>91</sup> Filtering software cannot only block certain "x"-rated sites (or restrict a user to sites that have been rated decent<sup>92</sup>), but also can prevent the use of "inappropriate" search terms to access unrated content.<sup>93</sup> Moreover, some filtering software products keep a log of attempted violations.<sup>94</sup> Despite these variations, three primary methods of filtering content can generally be discerned: (a) ratings-based blocking or "tagging"; (b) search-term blocking; and (c) image filtering. None are exceptionally effective at restricting minors' access to indecent material.

a) Ratings-based blocking/tagging

Ratings can be either self-imposed or issued by third parties, but both methodologies are similarly problematic. Self-rating involves the voluntary or mandatory rating of content by a web-site administrator,<sup>95</sup> while third party rating would involve some rating "authority." Both methods would require filtering software queued to the protocol of the particular rating system.<sup>96</sup>

---

91. See *ACLU*, 929 F. Supp. at 838-39 (discussing PICS). Some filtering software is already compatible with PICS. See *id.* at 840 (Cyber Patrol); see also Shapiro, *supra* note 90, at 118 ("Browser kings Netscape and Microsoft have said they will rely on PICS, a technical protocol that allows for easy and effective labeling and blocking of content.").

92. For example, the search engine "Yahoo!" offers a "kid-safe" version called "Yahooligans!" that retrieves only pre-approved sites, and can be accessed at <<http://www.yahooligans.com>>.

93. See Kubota, *supra* note 75, at 696; Black, *supra* note 77, at 21 (explaining the features of five different filtering products).

94. See Black, *supra* note 77, at 21.

95. A mandatory system of self-rating would likely be held unconstitutional after *Reno*. First, the problems involved in categorizing speech would make a statute mandating self-rating arguably vague; as one commentator put it, "[s]elf-rating would be subjective and annoying, and it would impose a frigid chill on free expression." See Shapiro, *supra* note 90, at 118. The trial court also considered the constitutionality of mandatory self-rating. It concluded that self-rating would be "extremely burdensome" for many Internet speakers, and that its "feasibility and effectiveness" had not been established. See *ACLU*, 929 F. Supp. at 847.

96. See *ACLU*, 929 F. Supp. at 848; Kubota, *supra* note 75, at 701-02. Such a system would work by embedding a string of characters in the URL or HTML, see *ACLU*, 929 F. Supp. at 847, or through the creation of a new top-level domain name such as ".xxx". The Generic Top-Level Domain Society, the entity charged with the creation of new top-level domain names, see Heather Mewes, *Memorandum of Understanding on the Generic Top-Level Domain Name Space of the Internet Domain Name System*, 13 BERKELEY TECH. L.J. 235 (1998), is considering and taking public comments on just such a proposal.

One problem with ratings-based blocking is that it invites censorship. Currently, rating of content on the Internet is performed primarily by the private companies that make and sell filtering software. It has been argued that allowing software makers to exert such power over the receipt of speech has, ironically, imposed a greater burden on First Amendment values than the CDA.<sup>97</sup> However, the decision to purchase and employ filtering software is voluntary, and no First Amendment values are threatened by a personal decision to forgo the receipt of certain types of speech. A more real threat to First Amendment values occurs when the standards used to identify and rate indecent content are not disclosed to the user of a filtering product. For example, a filtering product could block access to all sites that involve "abortion" or "family planning." Though such censorship is acceptable if consumers are aware of its existence, software designers arguably should be required to divulge their filtering criteria. However, the highly complicated nature of filtering programs makes it unlikely that users will fully understand the filtering criteria even if divulged. These problems are exacerbated when a governmental actor employs the software.<sup>98</sup>

Another problem with ratings-based blocking is that, depending on the methodology involved, access to Internet materials will be either under- or over-inclusive.<sup>99</sup> Filtering software using a ratings-based system can either (a) only allow access to rated sites, or (b) not allow access to rated sites. The first methodology excludes too much speech by restricting the materials available on the Internet to those that have been positively rated—that is, there are a multitude of "childsafes" sites that would be excluded under such a system.<sup>100</sup> The second methodology excludes too little content; material "harmful to minors" will still be accessible because such material will often be found on unrated sites. On balance, although ratings-based software continues to become a more effective tool for blocking content "harmful to minors," problems associated with the rating process will prevent ratings-based blocking from providing the "global" solution to Internet content sought by the CDA.

---

97. See Amy Harmon, *Technology to Let Engineers Filter the Web and Judge Content*, N.Y. TIMES, Jan. 19, 1998, at C1.

98. See Kubota, *supra* note 75, at 710-14 (applying rationale of book-banning cases to public school's use of filtering software).

99. See *id.*, at 697-703 (discussing methodologies).

100. Note, however, that the more prevalent this methodology is, the greater incentive content providers will have to self-rate, because otherwise they will not be able to reach those using the software.

b) Search term blocking

Most filtering products incorporate a method of preventing searches for indecent material.<sup>101</sup> For example, such software might prevent a search for "sex," and so prevent a user from retrieving links to "sex"-related sites. This "if you can't find it you can't see it" methodology is only partially effective. First, search term blocking does not prevent access to sites whose addresses are already known. Moreover, as noted above, seemingly innocuous search terms often lead to pornographic links.<sup>102</sup> Thus search term blocking does not provide a significant bar to minors' access of on-line indecency.

c) Image recognition

Another type of filtering software, which was not discussed in either the district court's or Supreme Court's opinion, is image recognition software. Image recognition is still a nascent field,<sup>103</sup> but such software is likely to become a viable method of information retrieval, as well as a helpful supplement to traditional text-based searching.<sup>104</sup>

Three methods of image recognition have been employed. The first works by comparing a sample image to other images in order to find similar images.<sup>105</sup> This method is "limited to finding superficially related images," and "is not very useful."<sup>106</sup> The second relies on the general appearance of the image—its "regions of near-constant color and texture" or the "stuff" that makes it up.<sup>107</sup> Such software can be fairly successful at image recognition, and a variety of programs have been developed using a "stuff"-based methodology.<sup>108</sup> The third methodology searches directly

---

101. See Black, *supra* note 77, at 21 (describing methods employed by six filtering products).

102. See *supra* note 70 and accompanying text.

103. See David Forsyth, et al., *Searching for Digital Pictures*, 276 SCIENTIFIC AMERICAN 6, 72 (1997) ("Unfortunately, current understanding of how to recognize objects in images falls far short of [its goal].")

104. "Ultimately, it should be possible to obtain a picture of a pouncing leopard by simply filling in a form ("spotty," "feline body plan," "leaping"), submitting it to a search engine and waiting for a selection of appropriate pictures to come back. This goal is achievable." *Id.* at 77.

105. See *id.* at 72.

106. *Id.* at 73.

107. *Id.* Thus a search for a sailboat might require specifying a large region of blue with a small region of yellow.

108. IBM (Query by Image Content) and MIT (Photobook) researchers have developed such programs. See *id.* However, proponents of the third methodology have argued that "stuff" based searching is still plagued by a variety of problems which will make it unable to "provide a sufficient foundation for content-based retrieval." *Id.* at 73-74.

for objects, such as horses or water, though it may also include “stuff”-based searching as a supplement. It is both the most promising from an information retrieval perspective, and the most difficult to implement.<sup>109</sup>

Image recognition technology can be applied in a filtering context. Nudity, in fact, is rather easy to detect because “skin has a very limited range of colors, and essentially no texture,” and because the body has a rather distinct “spatial layout.”<sup>110</sup> At least one object recognition program has been developed that identifies nudity with a fair amount of regularity.<sup>111</sup> As image recognition technology progresses, it may become a rather effective method of filtering content on the Internet. But image recognition software is still highly developmental, and its eventual effectiveness cannot yet be determined.

#### IV. CONCLUSION

Neither “low-tech” regulation, nor verification, nor filtering software bars minors’ access to harmful on-line content as effectively as would the CDA. Low-tech regulation will not provide a significant bar to minors’ receipt of on-line content because minors’ usage will be too difficult to monitor. Similarly, verification methods are costly, restrictive, and somewhat ineffective. While filtering technologies are better at blocking unwanted content than the other two methods, problems associated with the various types of filtering software leave it less effective than the CDA would have been. So, under the Court’s strict-scrutiny “alternatives” test, whereby a statute is held facially invalid if less restrictive alternatives that are *at least as effective* could be employed in furthering the governmental interest served by the statute,<sup>112</sup> the CDA should have been upheld.<sup>113</sup> As

---

109. See *id.* at 73-77. The most pressing difficulty is that of “perceptual grouping”—grouping relevant regions and shapes together for analysis.

110. David Forsyth & Margaret Fleck, *Finding People and Animals Using Body and Action Plans* (visited Dec. 1, 1997) <<http://http.cs.berkeley.edu/~daf.html>>.

111. See Forsyth, *supra* note 103, at 76-77 (“The program finds nude people in 40 percent of those images that contain them and in only 4 percent of those that do not.”); see also David A. Forsyth & Margaret Fleck, *Finding Naked People*, INT’L J. COMPUTER VISION (forthcoming 1998) (currently available at <<http://http.cs.berkeley.edu/~daf.html>>).

112. See *Reno v. ACLU*, \_\_\_ U.S. \_\_\_, 117 S. Ct. 2329, 2347-48 (1997).

113. This suggests some questions: First, will such alternatives be available in the near or distant future? It is possible that a combination of verification and emerging filtering technologies will eventually provide an adequate bar to minors’ access of harmful content, but that is an open question. Second, *should* the “less restrictive alternatives” test require that the alternative be “at least as effective,” or merely that they be “nearly” or “substantially” as effective? Volokh argues that the *Reno* decision demonstrates the

Eugene Volokh notes, "fairly effective, reasonably effective, not too awfully ineffective" alternatives are available, but no present method of content regulation is *as effective* as the CDA. Thus "the Court is, on the facts, simply wrong."<sup>114</sup> Whether this is viewed as a fatal error or fortuitous oversight, a survey of available methods of Internet content regulation demonstrates that the Court's factual assertion is indeed incorrect.

*Reno v. ACLU* is most notable for holding the Internet subject to the most stringent degree of First Amendment protection. This finding will severely limit governmental involvement in regulating content on the Internet, and so force the development of private regulatory measures. Though a variety of tools are currently available for the private regulation of Internet content, and more effective tools are being developed, no method currently available is likely to block minors' receipt of "harmful" on-line content as effectively as the CDA. The Court's decision in *Reno*, which assumes that there are *effective* alternatives, is therefore based on a factually incorrect finding. Nevertheless, responsibility for Internet content regulation has been decisively shifted to the private sector.

---

poverty of the less restrictive alternatives test, but also criticizes a "nearly as effective" approach, advocating instead a "balancing" approach. See Volokh, *supra* note 60, at §§ 2-4.

114. *Id.* at § II(A). Volokh does not consider the full gamut of methods available to regulate Internet content, concentrating instead on those specifically considered by the Court.