

Least Restrictive Means: A CLEAR PATH FOR USER-BASED REGULATION OF MINORS' ACCESS TO INDECENT MATERIAL ON THE INTERNET

I. INTRODUCTION

The First Amendment guarantees to Americans the freedom to communicate or express themselves in a public forum.¹ Such a principle of free expression will permit both elevated, and unfortunately, unelevated forms of communication in American society. Of course, there are exceptions to the First Amendment's grant of free speech. One exception focuses on protecting minors from harmful or indecent forms of communication.² Society recognizes that some forms of communication that are suitable for adults are not suitable for minors who lack maturity and emotional development.

Prior to the 1990s, legislators had been effective at drafting statutes that prevented minors from obtaining access to harmful forms of communication, while preserving adult access to such communication, thus avoiding a violation of the First Amendment.³ For instance, in *Ginsberg v. New York*, the Supreme Court upheld a New York statute that prohibited the sale of pornographic material to those under the age of seventeen.⁴ Although appellant challenged the constitutionality of the statute, the Supreme Court upheld it because, even though minors were not given access to pornographic material, adults could still obtain such material if they wished.⁵ Thus, *Ginsberg* places a burden on New York merchants who sell pornographic magazines to make certain they do not sell to minors.⁶ Such a burden is reasonable because shop owners can observe the persons to whom they sell pornographic material since such transactions take place in the context of the physical world, characterized by "geography" and "identity."⁷

In the 1990s, however, a new frontier has emerged in which throngs of people are interacting with one another, not in the physical world, but in the "electronic world"

1. See U.S. CONST. amend. I: "Congress shall make no law . . . abridging the freedom of speech . . ."

2. See *Ginsberg v. New York*, 390 U.S. 629, 636-639 (1968).

3. See *id.* at 633-34.

4. See *id.*

5. See *id.* at 634.

6. See *id.* at 631-32.

7. See *Reno v. American Civil Liberties Union*, 521 U.S. 844, 889 (1997) [hereinafter *Reno II*]. (citing Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 886 (1996)).

known as the Internet.⁸ As Justice O'Connor asserts in *Reno II*, "The electronic world is fundamentally different [than the physical world]. Because it is no more than the interconnection of electronic parties, cyberspace allows speakers and listeners to mask their identities."⁹ Indeed, the Internet has particularly heightened minors' access to pornographic material causing the government to argue, "With as many as 8,000 sexually explicit sites on the World Wide Web alone . . . the Internet threatens to render irrelevant all prior efforts to protect children from indecent material."¹⁰ Although somewhat hyperbolic, the government's fears certainly highlight an emerging problem: How can American society prevent minors from obtaining access to indecent material on the Internet while maintaining adult access to such material?¹¹

Part I will examine how Congress has attempted to solve the problem of minors' access to indecent material on the Internet through the passage of legislation, which will be followed by an analysis of the factors which account for the legislation's failure. Congress's first legislative attempt was Title V of the Telecommunications Act known as the "Communications Decency Act" ("CDA").¹² Congress's second legislative attempt was the "Child On-Line Protection Act" ("COPA").¹³ The CDA was held unconstitutional by the Supreme Court for violating the First Amendment¹⁴ and the COPA was enjoined by the Third Circuit for its likely violation of the First Amendment.¹⁵

Part II will examine alternative approaches to prevent minors' access to harmful communication on the Internet measured against the Supreme Court's analysis of the CDA and the Third Circuit's analysis of the COPA. One alternative approach would be to have speakers, commercial and non-commercial, regulate themselves through the use of adult identification pass codes or through a credit card number ("speaker-based regulation"). The other alternative would require parents to use protective software to regulate minors' access to harmful sites on the Internet ("user-based regulation"). User-based regulation successfully deals with the deficiencies of the CDA and COPA, without significant drawbacks.¹⁶ Speaker-based regulation, however, contains many of the same problems associated with the CDA and COPA.

8. See *id.* at 850. The Court found that, "About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999." *Id.*

9. *Id.* at 889.

10. Transcript of Oral Argument at 3, 1997 U.S. TRANS. Lexis 40, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (No. 96-511) (Mar. 19, 1997).

11. This paper does not argue against Congressional regulation of material on the Internet that is not protected under the First Amendment as to both adults and minors, such as, child pornography and obscenity.

12. 47 U.S.C. §223 (1994).

13. 47 U.S.C. § 231 (1994 & Supp. IV 1998).

14. See *Reno II*, 521 U.S. at 884.

15. See *American Civil Liberties Union v. Reno*, 217 F.3d 162, 181 (2000) [hereinafter *Reno III*]. See Miller, L. Heather, Note, *Strike Two: An Analysis of the Child Online protection Act's Constitutional Failures*, 52 FED. COMM. L.J. 155 (1999), for an examination of the CDA and/or COPA's constitutional failure in the federal courts.

16. See Harvard Law Review Association, *Internet Regulation Through Architectural Modification: The Property Rule Structure of Code Solutions*, 112 HARV. L. REV. 1634, 1639-1643, for an examination of some pros and cons of private filtering software.

II. THE CDA AND COPA

A. The CDA

Congress's first attempt to regulate minors' access to harmful material on the Internet was through two provisions of the CDA.¹⁷ In *Reno II*, the Supreme Court had the opportunity to examine the constitutionality of the two provisions of the CDA.¹⁸ The Court summarized the two provisions: "§ 223 (a)(1)(B)(ii) criminalizes the 'knowing' transmission of 'obscene or indecent' messages to any recipient under 18 years of age"¹⁹ (known as the "indecent transmission" provision) and § 223 (d) "prohibits the knowin[g] sending or displaying to a person under 18 of any message 'that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs . . .'" (known as the "patently offensive display" provision).²⁰

After distinguishing several cases put forth by the government in support of its position, the Court faults the CDA for using two different and undefined standards upon which to identify the prohibited communication.²¹ The CDA's failure to define "indecent" and "patently offensive" leaves those who communicate on the Internet uncertain as to the meaning of those terms and uncertain as to the relation, if any, those terms have to each other.²² The Court inquires, "[c]ould a speaker confidently assume that a serious discussion about birth control practices, homosexuality . . . or the consequences of prison rape violate the CDA?"²³ The Court held that this linguistic ambiguity, considered in addition to the criminal sanctions imposed for violations of the CDA, would serve to hinder or "chill" speech on the Internet because speakers would withhold potentially indecent communication, rather than risk a violation of the CDA.²⁴ This chilling of speech on the Internet is of serious constitutional concern because the CDA regulates content.²⁵ Regulation of speech based on content is subject to strict scrutiny analysis which requires a tight nexus between the government's purpose and the means by which the government attempts to achieve its purpose.²⁶ The Court held:

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. 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

17. See 47 U.S.C. §223(a)(1)(B)(ii) (1994 & Supp. IV 1998), 47 U.S.C. § 223(d) (1994 & Supp. IV 1998).

18. See 521 U.S. 844 (1997).

19. *Id.* at 859.

20. *Id.* at 859-60.

21. See *id.* at 871.

22. *Id.* The Court found that "indecent" does not, "benefit from any textual embellishment at all," and that "patently offensive" is qualified only to the extent that it involves "sexual or excretory activities or organs" taken "in context" and "measured by contemporary community standards." *Reno II*, 521 U.S. at 871 n.35.

23. *Id.* at 871.

24. See *Reno II*, 521 U.S. at 872.

25. See *id.* at 871.

26. See, e.g., *Schaumburg v. Citizens for a Better Environment*, 444 U.S. 620, 637 (1980).

to one another.²⁷

Here, the Court demonstrates its unwillingness to risk blocking adult access to speech that will likely follow from the vague provisions of the CDA.

Applying the CDA to the Internet's unique structure would also inhibit adult access to constitutionally protected speech. The Supreme Court, quoting the district court, found, "that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults."²⁸ The Court further held, the district court found "no effective way to determine the age of a user who is accessing material through e-mail, mail explorer, newsgroups, or chat rooms."²⁹ Here, the Court wholly debunks Congress's attempt to regulate through statutory provisions by asserting that the CDA is unworkable because, in many cases, it is not possible to determine the age of Internet users. Thus, the only effective means of denying minors access to indecent communication would be to deny access to everyone.

There are other reasons, albeit less noticeable, that account for the CDA's failure. The Court seemingly possesses a bias against regulation on the Internet; favoring instead, private regulation through protective software.³⁰ The Court held, ". . . [t]he [CDA's] burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the Act's legitimate purpose that the statute was enacted to preserve."³¹ Here, the Court intimates that Congress should yield to parental regulation of the Internet because it will be less restrictive than a statute that bases its preclusion of speech on cryptic standards. Additionally, the Court held that there is no indication that protective software would be less effective than statutory regulation.³² Also, the Court indicates that parents, under the CDA, could not allow their children to view material on the Internet that is patently offensive or indecent even if the parents believe the material has redeeming value.³³

The Court's bias against top down regulation on the Internet is also evident in a section of the case devoted to an explanation of the Internet.³⁴ This section demonstrates the Court's awe of this new medium's exponential growth and unparalleled opportunity to bring millions of people together through electronic communication.³⁵ For example, the Supreme Court, citing the district court, held, "at any given time 'tens of thousands of users are engaging in conversations on a huge range of subjects.' It is 'no exaggeration to conclude that the content of the Internet is as diverse as human

27. *Reno II*, 521 U.S. at 874.

28. *Id.* at 876 (citing *ACLU v. Reno*, 929 F.Supp. 824, 845 (E.D. Pa., 1996) [hereinafter *Reno I*]).

29. *Id.*

30. *See Reno I*, 929 F.Supp. at 877-884. Judge Dalzell makes a compelling argument that the unique characteristics of the Internet make regulation of it difficult if not impossible. Indeed, in support of his stance against the government's attempt to regulate the Internet through the CDA, he asserts, "Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects." *Id.*

31. *Reno II*, 521 U.S. at 874.

32. *See id.*

33. *See id.* at 878.

34. *See id.* at 850-52.

35. *See id.*

thought.”³⁶ Here, the Court exposed its psyche showing that it holds the Internet in such high esteem that it describes it like no other medium; one that is tantamount to the complexity and diversity of the human mind. After such an assertion, it seems unlikely that the Court would impede this novel and useful medium through broad regulation.

Another indication that the Court is biased against Congressional regulation of the Internet is the Court’s comparison of the Internet to the broadcast medium.³⁷ The Court held that the broadcast medium was subject to an extensive history of past regulation.³⁸ In contrast to the broadcast medium, the Court held, “[n]either before nor after the enactment of the CDA have the vast democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry.”³⁹ In the above excerpt, by stating that the Internet has not been subject to extensive regulation, the Court is implying that it is unwilling to regulate it now. Of course, this reasoning is tautological; a new medium will never be regulated if courts preclude its regulation based on the principle that it has not yet been regulated. Thus, the Court is even willing to engage in circular reasoning to justify its refusal to regulate the Internet. Moreover, in the same excerpt, the Court describes the Internet as democratic; a word that contains a positive aura of liberty which stands in contrast to government regulation.

In its review of the CDA the Court does not conjecture that perhaps the statute would pass constitutional muster if technological advances made it possible and economical to determine the ages of Internet users.⁴⁰ Instead, the Court advocated a new course of regulation through parental control when it held, “[b]y contrast, the District Court found that ‘[d]espite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available.’”⁴¹ In other words, the Court is indirectly telling Congress to relinquish its legislative efforts to prevent minors from accessing harmful material on the Internet that adults have a protected right to view because parental control software will soon supplant the perceived need for statutory regulation.

B. COPA

Congress’s second attempt to regulate minors’ access to the Internet was through the Child Online Protection Act (“COPA”), which prohibits any person from, “knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to

36. *Id.* at 852 (quoting *Reno I*, 929 F.Supp. at 842).

37. *See Reno II*, 521 U.S. at 867.

38. *See id.*

39. *Id.* at 868-69 (citation omitted).

40. *See id.* at 889. Justice O’Connor, however, in her concurring and dissenting opinion, indicates that she would uphold a regulation of the Internet based on effective zoning insofar as it does not interfere with the First Amendment Rights of Adults. *See id.* O’Connor also states that the Court reviewed the CDA in the context of the Internet as it existed at the time of *Trial*. *See id.* However, the Court did not go out of its way to suggest that it would uphold Congressional regulation even if technology made it feasible.

41. *Id.* at 877 (citing *Reno I*, 929 F.Supp. at 842).

minors.”⁴²

Upon passage of the COPA, the American Civil Liberties Union filed for an injunction against its enforcement, which was granted by the district court.⁴³ On appeal, the issue came before the Third Circuit in *American Civil Liberties Union v. Reno* (“*ACLU*”).⁴⁴ The court noted that Congress attempted to draft COPA more narrowly than the CDA by limiting its coverage to “material on the web as opposed to the Internet as a whole” and to commercial communication.⁴⁵ The court also acknowledged that the government attempted to clear up the linguistic ambiguity, which engendered the CDA’s demise under the First Amendment, by limiting the measure of prohibited communication to that material which is “harmful to minors.”⁴⁶

The “harmful to minors” standard could only be met if the communication satisfied a three-part test that was modified from *Miller v. California*.⁴⁷ Thus, harmful to minors under the COPA is defined as §231(e)(6) “any communication . . . that is obscene or that – (A) the average person, applying contemporary community standards, would find . . . is designed to appeal to, or is designed to pander to, the prurient interests;”⁴⁸ (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or stimulated sexual act or sexual contact . . .”⁴⁹ (C) “taken a whole, lacks serious literary, artistic, political, or scientific value for minors.”⁵⁰ This three-part test was incorporated into COPA for the express purpose of overcoming the vagueness associated with Congress’s failure to define the “indecent transmission” provision⁵¹ and the “patently offensive display” provision⁵² of the CDA.⁵³ The main problem with Congress’s strategy, however, was that by incorporating the *Miller* factors into COPA, it, in effect, attempted to apply a test to the electronic world that was designed to regulate the physical world. The Court acknowledged that Congress was aware that applying a community standards test that was designed for the physical world as a means to measure prohibited communication in the electronic world was “controversial.”⁵⁴ The government contends, however, that, “there is nothing dispositive about the fact that [in COPA] commercial distribution of such [harmful] materials occurs through an online, rather than a brick and mortar outlet.”⁵⁵ Nonetheless, the Court expressed disagreement with the government’s contention that the electronic world could be reconciled with the physical world through a non-geographic test for material

42. *American Civil Liberties Union v. Reno*, 217 F.3d 162, 167 (2000) (citing 47 U.S.C. §231 (a) (1)) [hereinafter *Reno IV*].

43. *See id.* at 165-66.

44. *See id.*

45. *Id.* at 167.

46. *See id.* at 167.

47. *See id.* at 167 (citing *Miller v. California*, 413 U.S. 15 (1973)).

48. 47 U.S.C. § 231(e)(6)(A) (1994 & Supp. IV 1998).

49. 47 U.S.C. § 231(e)(6)(B) (1994 & Supp. IV 1998).

50. 47 U.S.C. § 231(e)(6)(C) (Supp. IV 1998).

51. *See* 47 U.S.C. § 223(a) (Supp. II 1994).

52. *See* 47 U.S.C. § 223(d) (Supp. II 1994).

53. *See Reno IV*, 217 F.3d at 167-68.

54. *See id.* at 174 (citing H.R. REP. No. 105-775, at 28 (1998)).

55. *Id.* (citing Brief for Appellant at 18 n. 3, *American Civil Liberties Union v. Reno*, 217 F.3d 162 (2000)).

that is harmful to minors.⁵⁶

The Court held that the key difference between the Internet and the physical world is the existence of boundaries.⁵⁷ In the physical world, there is a clear demarcation between the point at which one geographical location begins and at which it ends; whereas the Internet is essentially without such boundaries.⁵⁸ In *Miller*, the Court upheld a statute that required the appellant to alter the content of the material he was mailing depending on the standards of the recipient's community because he had control over what communities would receive his materials.⁵⁹ In contrast, a dispenser of material on the Internet cannot control who will gain access to the material because the Internet is without boundaries.⁶⁰ Communicators on the Internet cannot refuse access to selected areas because such segments or partitioned areas do not currently exist.⁶¹ Indeed, the Third Circuit held that because communicators on the Internet cannot control whom their communications will reach they will be forced to communicate at the standard set by the most conservative community.⁶² Thus, applying a community standards test to an electronic world lacking distinct communities can only be effectual if the legal system creates an artificial, monolithic community, incorporating all geographic areas that have access to the Internet. This effectively amounts to totalitarian governance of the Internet by the community espousing the most prudent values; hardly the democratic enterprise described by the Supreme Court in *Reno II*.⁶³

The government attempted to preserve the CDA and COPA from the "strong medicine"⁶⁴ of the First Amendment by inserting affirmative defenses into both statutes. The CDA gives an affirmative defense to those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications.⁶⁵ The CDA also offers an affirmative defense to those who require proof of age through an adult identification number or code or credit card.⁶⁶ The COPA has a similar affirmative defense provision which provides that if a Web publisher, "has restricted access by minors to material that is harmful to minors through use of a credit card . . . adult personal identification number . . . then no liability will attach to the web publisher even if a minor should nevertheless gain access to the restricted material under COPA."⁶⁷ By inserting these provisions into both statutes the government intended to encourage web communicators dispensing indecent material to block minors' access. Nevertheless, the Supreme Court in *Reno II* held that installing such age verification technology would be prohibitively costly and burdensome for noncommercial

56. *See id.* at 174-75.

57. *See id.* at 175 (citing *ACLU v. Reno*, 31 F.Supp.2d 473, 482-92 (E.D. Pa., 1999) [hereinafter *Reno III*]; *See American Libraries Association v. Pataki*, 969 F.Supp. 160, 169 (S.D. NY, 1997) which states that "geography, however, is a virtually meaningless construct on the Internet.").

58. *See id.*

59. *See Reno IV*, 217 F.3d at 175.

60. *See id.* (citing *Reno III*, 31 F.Supp.2d at 484).

61. *See id.*

62. *See id.* at 177 (citing *Reno II*, 521 U.S. at 877-78).

63. *See Reno II*, 521 U.S. at 867.

64. *Reno IV*, 217 F.3d at 177 (citing *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973)).

65. *Reno II*, 521 U.S. at 844 (citing § 223(e)(5)(A)).

66. *See id.*

67. *Reno IV*, 217 F.3d at 170 n.14 (citing 47 U.S.C. § 231(c)(1)).

speakers.⁶⁸ Moreover, commercial providers of indecent material even with identification requirements could not be certain that minors were sufficiently precluded from gaining access to their sites, thus rendering such identification measures irrelevant.⁶⁹ Indeed, the Supreme Court held, “[T]he government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults.”⁷⁰ In other words, age verification systems do not work well enough to satisfy the government’s interest of protecting minors from indecent material on the Internet.

Perhaps the greatest argument against the CDA and COPA involves their limited jurisdiction. The CDA and COPA may prevent Internet speakers in the United States from exposing minors to indecent or patently offensive communication, but they would not prevent foreign communicators from doing so because they do not fall within the purview of the statutes.⁷¹ During oral argument in *Reno II*, appellee estimated that fifty percent of indecent speech in cyberspace is posted in foreign countries.⁷² Thus, even assuming that the CDA and COPA effectively prevented minors from obtaining access to harmful materials posted in the United States, minors would still have access to a plethora of indecent speech posted in foreign countries.⁷³ Moreover, the COPA only applies to commercial speakers, which leaves minors unprotected against noncommercial speakers.⁷⁴ In light of foreign postings under the CDA and COPA and noncommercial speakers under COPA, the government’s interest in protecting minors’ from indecent material on the Internet would not have been met. This reality led the Third Circuit in *ACLU*, to hold:

[E]ven if we were to overlook the unconstitutional overbreadth of the COPA “contemporary community standards” test and if COPA were to be deemed effective, it still would not eliminate much of the harmful material which a minor could access. For example, minors would still access harmful material published by non-commercial Web publishers, and by foreign web publishers.⁷⁵

Since Congress’s statutory attempts to prevent children from obtaining access to indecent material on the Internet failed strict scrutiny analysis, it is important to consider alternative approaches. Two alternatives are speaker-based and user-based regulation which will be considered in turn.

III. SPEAKER-BASED VERSUS USER-BASED REGULATION

A. Speaker-Based Regulation

Speaker-based regulation places the onus on those who disseminate or display

68. See *Reno II*, 521 U.S. at 881-82.

69. See *id.* at 882.

70. *Id.*

71. See *Reno IV*, 217 F.3d at 177 n.21.

72. Transcript of Oral Argument at 52, 1997 U.S. TRANS. Lexis 40, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (No. 96-511) (Mar. 19, 1997).

73. *Reno IV*, 217 F.3d at 177 n.21.

74. See *id.* at 167.

75. *Id.* at 177 n.21.

material on the Internet to screen out minors through identification codes, credit card numbers and other types of profiling. In *Reno II*, Justice O'Connor describes speaker-based regulation as a species of adult zoning on the Internet.⁷⁶ Justice O'Connor writes,

[I]t is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world, and consequently more amenable to zoning law...Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves . . . before they can access certain areas of cyberspace.⁷⁷

Despite Justice O'Connor's apparent enthusiasm for speaker-based regulation, it is important to note that speaker-based regulation poses a similar threat to the democratic structure of the Internet as do the COPA and CDA. As previously mentioned, installing such systems would be costly for speakers, especially noncommercial speakers who would perhaps be rendered mute by such a legislative demand for speaker-based regulation.⁷⁸ Although adult identification PINS are considerably less expensive than credit card verification, both types of regulation require a reorganization and maintenance fee.⁷⁹ Thus, the costs and inconvenience of such a system may dissuade some speakers from using the Internet, which, like the CDA and COPA, would effectively deprive adults of protected speech.

Speaker regulation prevents adult access to constitutionally protected material on the Internet in other ways as well. The Third Circuit in *ACLU* held:

[B]oth credit card and age verification systems require an individual seeking to access material otherwise permissible to adults to reveal personal statistics. Because many adults will choose not to reveal these personal details, those otherwise frequently visited Web sites will experience "a loss of traffic." This loss of traffic in turn would "inflict economic" harm upon the particular website.⁸⁰

Here, two problems with communicator regulation are highlighted by the Court. First, the embarrassment and shame of revealing personal information prior to entering an indecent site will cause many adults to avoid such sights.⁸¹ Thus, identification measures will preclude adult access to protected speech.⁸² Although this preclusion is psychological, rather than legal, it still produces the same undesired effect of preventing adults from accessing protected speech in cyberspace.⁸³ Second, the reduction in traffic

76. See *Reno II*, 521 U.S. 844, 890 (1997).

77. *Id.*; See also, Transcript of Oral Argument at 7, 1997 U.S. TRANS. Lexis 40, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (No. 96-511) (Mar. 19, 1997). Appellees assert that most web sites, including the "12 million . . . who gain access through . . . the major online service providers" do not have CGI Script, which is necessary to screen for age. *Id.* Thus, Justice O'Connor's assertion that the Internet can be zoned to emulate the physical world has yet to be proven sufficiently workable. Moreover, in the physical world speakers are visible; in the electronic world speakers are not visible. Hence, it seems unrealistic to assume that CGI Script will magically make screening minors on the Internet as efficient as screening minors in the physical world. Lastly, even if it were the case that the Internet could be zoned to emulate the physical world, would not such an outcome spoil the unique, amorphous medium the world has come to revere?

78. See *Reno IV*, 217 F.3d at 170-71 (citing *Reno I*, 929 F.Supp. at 490).

79. See *id.*

80. *Id.* (citing *Reno I*, 929 F.Supp. at 461).

81. See *id.*

82. See *id.*

83. See *id.*

will hurt the business of commercial speakers increasing the likelihood that they will shut down, thus depriving adult access to protected speech.⁸⁴ Thus, speaker-based regulation fails to sufficiently deal with the main problem confronting the CDA and COPA, that is, the maintenance of adult access to constitutionally protected material on the Internet.

B. User-Based Regulation

Protective software, such as Net Nanny and Cyber Patrol, presents a viable alternative to the dangers of Congressional regulation.⁸⁵ Protective Software will prevent the browser from downloading content deemed inappropriate for minors by either the software company or parents.⁸⁶ The software can be periodically updated to counter the Internet's rapid growth.⁸⁷ The primary benefit of protective software is that it does not suffer from the deficiencies of the CDA and COPA. First, protective software does not prevent adults from gaining access to indecent material on the Internet because it is a privately, rather than, a governmentally controlled measure. Adults can override denial of access by use of a password.⁸⁸ Second, the success of privately maintained software does not depend on the illusive task of erecting untenable artificial borders on the Internet. Third, private software is not as costly to the individual user as identification systems are to speakers.⁸⁹ Fourth, private software would effectively close up the foreign posting loophole.⁹⁰ Fifth, private software allows parents, not the government as proscribed by the CDA, to determine what information on the Internet is suitable for their children.⁹¹ Most parents would favor this discretion in light of the fact that they are responsible for their children's development.

There are arguments against reliance on user regulation software. The government during oral argument in *Reno II* argued that such software will potentially block access to sites that are protected for minors.⁹² But as Appellee, rebutted, "[T]hat's not a First Amendment problem. That's a parental judgment issue."⁹³ Further, the government fails to explain how the CDA or COPA will not have the same effect. At least in user-regulated software the minors deprived of speech are from the class of people who engendered the need for regulation. Under the CDA and COPA, however, adults were

84. See *Reno IV*, 217 F.3d at 170-71.

85. See Jonathon Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J., 453-455 (1997).

86. See Commission on Child Online Protection (COPA), Report to Congress 21 (2000).

87. See *id.*

88. See *id.*

89. See Transcript of Oral Argument at 90, 1997 U.S. TRANS. Lexis 40, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (No. 96-511) (Mar. 19, 1997). Compare *Reno II*, 521 U.S. at 881-82. The cost to speakers of screening for minors would in many cases be prohibitive, thus precluding them from using the Internet. In contrast, the cost of private software to users would not be so great as to preclude them from using the Internet. Moreover, this could be an area of limited government intervention, in which, Congress could subsidize the purchase of private software for low-income families.

90. See *id.*

91. See *Reno II*, 521 U.S. at 878.

92. See Transcript of Oral Argument at 48, 1997 U.S. TRANS. Lexis 40, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (No. 96-511) (Mar. 19, 1997).

93. *Id.*

deprived of speech, even though the need for regulation did not transpire for their protection.

Another argument against user regulation is put forth by anti-pornography activists who assert that: “[S]uch software ‘leaves the parent . . . responsible to go out and buy the software, become educated about how to apply it, how to install it, how to use it, and how to then monitor it to make sure your child or his friends have not gotten around it.’”⁹⁴ Although this argument has some merit, the decision to use legislative regulation versus self-regulation should not rise or fall on the indolence of parents. Parenting is difficult in all facets of life, such as making sure children do not eat too much sugar. Even though children can surreptitiously obtain candy and eat it against parental wishes most Americans would not call for government regulation of children’s access to candy.

Another argument against user-based regulation is the glitches in the accuracy of protective software and the confusion over how the development of the next generation of software should proceed.⁹⁵ Although software protection has some problems, it will only improve with time. Indeed, “President Clinton has pledged to ‘vigorously support’ the development . . . of filtering software.”⁹⁶ Moreover, the Commission On Child Online Protection in its report to Congress stated that, “Voluntary methods and technologies to protect children must be developed, tested, evaluated and made readily available,”⁹⁷ and the commission further called for “greater use of existing technologies.”⁹⁸ Eventually, as shown with other burgeoning products, the most efficient and effective protective software will emerge through the natural process of the market economy. It would be more prudent to patiently wait for the second and third generation of protective software before allowing Congress to imprison the Internet through full-fledged regulation. Although there have been worthy arguments levied against user-based regulation, they do not rise to the level of seriousness as those arguments levied against legislative and speaker-based regulation. Perhaps Winston Churchill’s assertion about democracy best sums up the Internet regulation dilemma, that is, protective software is the worst form of Internet regulation, except for all the others.

IV. CONCLUSION

The overbreadth of the CDA and COPA, the unique borderless structure of the Internet that makes it nearly impossible to keep certain communications limited to some areas but not others, the economic burden of installing identification systems, and lack of jurisdiction over foreign speakers makes parental or self-regulation a more reasonable and workable solution to the problem of minors’ access to indecent speech on the Internet. However, there are certain things Congress can do to help which do not involve regulation of content. For example, Congress could subsidize local community efforts to train parents in the use of blocking software and require all Internet service providers to come equipped with blocking options that parents can employ with a click

94. Weinberg, *supra* note 86, at 482 n.2 (1997) (citing *Pornography on the Internet: Straight talk from the Family Research Counsel* (radio broadcast transcript) (last modified July 3, 1996)).

95. *See id.* at 459-470.

96. *Id.* at 454 (quoting presidential statement).

97. Commission on Child Online Protection (COPA), Report to Congress 21 (2000):

98. *Id.*

of the mouse.

It seems reasonable to take the responsibility to regulate away from those who do not have control over minors' access to material on the Internet, thereby placing it in the hands of parents. Asking web publishers or communicators to regulate that which they cannot is really asking them to close up shop. Most people would agree that American society is not ready to close off the Internet to a significant number of communicators, even if their communication is of a lower form. Congress should, therefore, relinquish its efforts to regulate communication on the Internet that is harmful to minors but protected as to adults in favor of parental or user-based regulation.

*Anthony Niccoli**

* B.A., Government and Philosophy, University of Notre Dame, 1996; Juris Doctor Candidate, Notre Dame Law School, 2001. I would like to thank my parents and Rose for their support in this endeavor and I would also like to thank Professor Patricia Bellia, Notre Dame Law School, for her helpful comments and suggestions.