Untangling the World Wide Web: Restricting Children’s Access to Adult Materials While Preserving the Freedoms of Adults

INTRODUCTION

Currently, some view the Internet as a fountainhead for anarchy, beyond the control of state or federal government. They view it as a wild frontier, and like the Wild West of early America, they seek to conquer and tame it before lawlessness abounds. Responding to these views, The United States Congress has already twice passed legislation in an attempt to restrict children’s access to the indecent material on the Internet. State legislatures have attempted to pass similar restrictions. The federal laws have encountered First Amendment difficulties when reviewed in court. In addition to First Amendment difficulties, state statutes in this area have run into Commerce Clause problems as well. Reasons given by the courts for these statutes’ conflicts with the First Amendment are several, including vagueness, overbreadth, and failure to pass strict scrutiny.
The first major U.S. Supreme Court case dealing with freedom of speech and the restriction of children's access to adult materials on the Internet was the landmark case of *Reno v. ACLU,* (Reno I) where the high Court struck down two provisions of the Communications Decency Act (CDA) as unconstitutional under the First Amendment to the U.S. Constitution. In response to the Court’s decision in *Reno I,* Congress passed the Child Online Protection Act (COPA), which it hoped would cure the constitutional deficiencies of the CDA. The American Civil Liberties Union, along with several others, immediately challenged the constitutionality of COPA, and the U.S. Court of Appeals for the Third Circuit also found this latest effort by Congress unconstitutional under the First Amendment. Many scholars feel that any criminal law like COPA will be found unconstitutional. In fact, the Third Circuit Court reviewing COPA itself suggested that any such criminal statute may run into First Amendment difficulties under the current state of computer technology. Yet, if the criminal statutes enacted so far are not the answer to the problem of free access by children to pornographic material, of speech will only be upheld if it is reasonably necessary to serve a compelling government interest and is narrowly tailored to achieve that government interest. *Carey v. Brown,* 447 U.S. 455, 461 (1980), *cited in Perry Education Ass’n v. Perry Local Educators’ Ass’n,* 460 U.S. 37, 45 (1983).

---

8. 521 U.S. 844.
13. Other plaintiffs included: Androgyny Books, Inc.; American Booksellers Foundation for Free Expression, Inc.; Artnet Worldwide Corporation; Blackstripe; Addazi, Inc.; Electronic Frontier Foundation; Electronic Privacy Information Center; Free Speech Media; Internet Content Coalition; Ohgyn.net; Philadelphia Gay News; Powell's Bookstore; Riotgrrl; Salon Internet, Inc.; and West Stock, Inc. *Reno III,* 217 F.3d at 162.
14. *See id.*
16. *See Reno III,* 217 F.3d at 166.

In affirming the District Court, we are forced to recognize that, at present, due to technological limitations, there may be no other means by which harmful material on the Web may be constitutionally restricted, although, in light of rapidly developing technological advances, what may now be impossible to regulate constitutionally may, in the not-to-distant future, become feasible.

*Id.*
then what are the alternatives? More generally, what is the future of laws attempting to regulate adult material on the Internet?

This comment attempts to shed some light on these questions by examining the current state of the law in the area of internet regulation restricting children's access to adult material. This area of law is very new, with the majority of case precedent developed over just the last five or six years. Although the term "Internet" applies to various aspects of cyberspace including the World Wide Web, e-mail, chat rooms, listserves, newsgroups, FTP's, and other interactive environments, this essay will focus mainly on the area of the World Wide Web. Part I of this comment provides a brief overview of the U.S. Supreme Court precedent relating to freedom of speech and various forms of media. Part II gives a description of the history, terminology, and characteristics of the World Wide Web. Part III gives a brief analysis of the CDA and the Reno I case. Part IV briefly discusses COPA and the Reno II and III cases. Part V analyzes four other early landmark cases involving government regulation of adult material on the Web. It also predicts the resolution in court of a COPA-like law under reliable geographic and age-verification technology, based on the current state of law derived from these four cases and the Reno decisions. It also discusses other possible future trends in this area of law through a critique of three other law review articles on this topic. Part VI will examine some alternatives to criminal statutes that may limit children's access to adult websites. Part VII concludes that future criminal laws like COPA will most likely not withstand First Amendment scrutiny, and that future attempts at governmental regulation of adult websites via criminal statutes will probably prove equally unsuccessful, at least until technology advances enough to allow for reasonable precision in restricting children's access while not stifling adults' freedom of speech on the Web.

I. OVERVIEW OF U.S. SUPREME COURT PRECEDENT

Before exploring the world of internet regulation, this comment will begin by briefly examining how the U.S. Supreme Court has viewed First Amendment protections of adult material in other forms of media including magazines, mail brochures, radio, adult theaters, telephone, and cable television communications. A brief overview of the following cases provides a background into the Supreme Court’s treatment of First Amendment protections and these forms of media.

17. See Reno I, 521 U.S. at 851.
A. *GINSBERG V. NEW YORK*\(^{18}\)

The Supreme Court ruled that a state statute that prohibited the sale of material "harmful to minors"\(^{19}\) did not infringe upon minors' constitutional freedom of expression and that the statute's definition of "harmful to minors" was not unconstitutionally vague.\(^{20}\) The Court found that a state may prohibit the distribution of sexually-explicit materials to children, even if those materials would not be considered obscene to adults.\(^{21}\)

B. *MILLER V. CALIFORNIA* \(^{22}\)

The Court held that obscenity is not a constitutionally protected class of speech.\(^{23}\) In determining whether matter is obscene, state courts should ask whether:

1) the average person, applying contemporary community standards, would find that the work, taken as a whole, appealed to the prurient interest; 2) the work depicted or described, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and 3) the work, taken as a whole, lacked serious literary, artistic, political, or scientific value.\(^{24}\)

In order to meet the requirement of finding material obscene, the state law must specifically define the sexual conduct or description that is prohibited so as to provide fair notice as to what is prohibited.\(^{25}\) The *Miller* Court ruled that

---

18. 390 U.S. 629 (1968). Defendant Ginsberg was convicted of violating a statute that prohibited the knowing sale of sexually explicit magazines to an individual under seventeen years of age. *Id.*
19. The statute defined "harmful to minors" as material that "appeals to the prurient interest of minors," is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors," and is "utterly without redeeming social importance for minors." *Id.* at 633.
20. *Id.* at 643-45. A statutory definition is not unconstitutionally vague if it gives adequate notice of what is prohibited. *Id.*
21. *Id.* at 636-37.
22. 413 U.S. 15 (1973). Miller was convicted for mailing unsolicited brochures, which contained pictures of explicit sexual acts in violation of a California statute making it a crime to knowingly distribute obscene material. *Id.*
23. See *id.*
obscenity is to be determined by applying "contemporary community standards," not a "national standard."26

C. FCC v. PACIFICA FOUNDATION 27

The United States Supreme Court held that the Federal Communications Commission (FCC) had the authority to impose sanctions on licensees who broadcast indecent material during hours in which children are likely to be a part of the audience.28 The Court found that such a restriction was not overbroad and the fact that the broadcast was not obscene did not prevent the FCC from prohibiting the broadcast when children were likely to be in the audience.29 Thus, the FCC could properly take context into account.30 While such indecent words would have a certain amount of First Amendment protection, the fact that indecent words were broadcast over radio at an early hour made the message accessible to children in the privacy of one's own home.31 Since broadcast radio is a "pervasive" medium, greater prohibition of speech than would normally be the case for indecent, as opposed to obscene, material is allowable.32 Radio has also traditionally been a heavily-regulated medium by the FCC. Such heavy regulation is justified because of the "scarcity" of the broadcast medium.33

D. NEW YORK V. FERBER34

The U. S. Supreme Court ruled that, like obscenity, child pornography is unprotected by the First Amendment if it includes a visual depiction of sexual conduct by children without serious literary, artistic, political, or scientific

26. Id. at 30.
27. 438 U.S. 726 (1978). The FCC held the owner of a radio station could be subject to administrative sanctions under 56 FCC 2d 94 for airing a monologue by comedian George Carlin in which Carlin uses the "seven words that you can never say on the public airwaves" during the early afternoon hours. Id.
28. See id.
29. See id at 746.
30. Id. at 747-48.
31. Id. at 746-49.
32. Id. at 748. Radio is a "pervasive" medium in that it enters the home of the listener without warning of the content.
33. Id. at 731 n.2. The broadcast medium is "scarce" because traditional broadcast receivers can only receive a limited number of transmissions in one area. If too many signals are broadcast in a single area, the signals will "interfere" with each other.
34. 458 U.S. 747 (1982). The defendant was the owner of a bookstore and was convicted for selling films, which contained images of young boys masturbating, in violation of a state statute that proscribed the knowing promotion of sexual performances by children under the age of sixteen. Id.
value. Child pornography is not constitutionally protected even if it is not obscene because of a compelling state interest in protecting children and preventing sexual exploitation and abuse of children.

E. RENTON V. PLAYTIME THEATERS

The United States Supreme Court held that a city zoning ordinance which prohibited adult theaters from locating within 1,000 feet of any residence, church, park, or school was a content-neutral restriction on speech, and that as a time, manner, and place restriction, the ordinance was not analyzed under the same strict scrutiny afforded to restrictions on the content of speech. The Court also found that the ordinance served a substantial governmental interest in curtailing the "secondary effects" of such adult establishments, such as potential increases in crime in the surrounding neighborhood. The majority felt that the ordinance allowed for reasonable alternative means of communication outside of the zoned area. The Court ruled that the city's ordinance was constitutional despite the fact that the individuals of the community would have to pay to enter the privacy of the establishment before they would be able to view any sexually-explicit material.

F. SABLE COMMUNICATIONS OF CAL., INC. V. FCC

The United States Supreme Court found that a total ban on obscene, interstate, commercial telephone communications did not violate the First Amendment because First Amendment protection does not extend to obscene speech. The majority felt that it did not matter that distributors of obscene telephone communications might be subjected to varying community standards in different federal districts in determining the obscenity of the material. The Court, however, did find the total ban on indecent telephone communications unconstitutional under the First Amendment, because of the denial of adult

35. Id. at 764.
36. Id. at 760-61.
38. Id. at 48-49.
39. Id. at 49.
40. Id. at 52.
41. See id.
42. 492 U.S. 115 (1989). Sable Communications, a company that offered sexually-oriented prerecorded telephone messages to customers who dialed into the company, challenged FCC prohibitions against indecent and obscene telephone messages. Id.
43. Id. at 124.
44. Id. at 124-25.
access to these telephone messages. Unlike the *Pacifica* case, which prohibited indecent broadcasts over radio, the receipt of indecent telephone communications requires “affirmative steps” on the part of the listener as opposed to the “pervasive” nature of the radio. Since telephone communications are not a pervasive medium in the way broadcast radio is, the Court found that the total ban was not the least restrictive means of serving the government interest of protecting minors from indecent phone communications so as to satisfy strict scrutiny under the First Amendment.

G. *DENVER AREA EDUCATIONAL TELECOMMUNICATIONS CONSORTIUM V. FCC*

Three provisions of the Cable Television Consumer Protection and Competition Act of 1992 were challenged. The Court found that no rigid judicial formulas can be applied to all media. A provision permitting cable operators to prohibit patently offensive, sexual material on leased channels was deemed constitutional because editorial speech is protected and the leased channels on cable are similar to broadcast radio in *Pacifica*, even though the viewer must first subscribe to cable. A provision that required cable operators to segregate patently offensive, sexual material to separate leased channels was found unconstitutional because less restrictive alternatives like lockboxes existed, and thus the provision did not survive the strict scrutiny of First Amendment review. A provision allowing cable operators to prohibit patently offensive, sexual materials from public access channels was also found unconstitutional because municipal supervisory control was more appropriate and less restrictive.

---

45. *Id.* at 131.
46. *Id.* at 127-28.
47. *Id.* at 128.
49. *See id.* The first provision allowed cable operators to ban indecent programming on leased channels. The second provision required cable operators to segregate indecent programming onto a single channel and block that channel unless the subscriber requested access to the channel in writing. The third provision allowed cable operators to prohibit indecent programming on public access channels. *Id.*
50. *Id.* at 741-42.
51. *Id.* at 743.
52. *Id.* at 760.
53. *Id.* at 766.
II. WORLD WIDE WEB

A. CHARACTERISTICS OF THE WORLD WIDE WEB

Before any discussion can begin about the state of the law relating to government regulation of the World Wide Web, not only is an understanding of speech and media case precedent important, but an understanding of the history, technology, usage, vocabulary, and characteristics of the Web is also necessary. The World Wide Web is part of the category known as the "Internet." The use of the Internet proliferated in the early 1990's and is now used as a means of communication by millions of people throughout the world. People can gain access to the Internet from a variety of sources usually via commercial hosts or universities. These commercial and non-commercial hosts are referred to as "Internet Service Providers" or "ISP's" and offer modem or cable access to a computer network linked to the Internet. Individuals can gain access to the Internet through ISP's for a relatively small fee or sometimes for free as a benefit of work, college, or group affiliation.

Once these individuals have access to an internet account, they can access the World Wide Web through the use of a "web browser" which allows them to "surf" various websites published by others. With the use of a browser such as "Netscape" or "Internet Explorer," individuals may view text, photos, video, and audio from these various websites. Each web page has its own specific address, and contains a hypertext transfer protocol, or "http." A web surfer may either type in a known web address directly or use a "search engine" to enter keywords. The search engine will then give the user a list of sites, and direct links to those sites, which contain the keywords entered by the web surfer. The Web also uses a formatting language called hypertext markup language, or "HTML," which allows the browsers to interpret and

54. Reno I, 521 U.S. at 849-50. The Internet is an international network of interconnected computers that began as a military program called "ARPANET" in 1969, and which later led to the rapid development of civilian networks. Id.
55. Zick, supra note 15, at 1155. "While estimates are difficult to confirm, the Internet is currently believed to connect more than 159 countries and over 100 million users." Id.
56. Reno I, 521 U.S. at 850.
57. Reno II, 31 F. Supp. 2d at 482. A modem is a piece of computer hardware that allows a user to access the Internet via a telephone line.
58. Id.
60. Id.
61. Id. The hypertext transfer protocol is the standard web formatting language. Id.
63. Reno I, 521 U.S. at 852.
display the information presented on the page. Websites usually contain “links” which allow the web surfer to access other sites directly from the site they are already viewing. Most websites are freely accessible to a web surfer, but some require a password or credit card number in order to proceed to the site or certain pages within the site. Most websites offer at least some free content as a way of creating greater “traffic” to the site. Adult sites often generate traffic to their sites by offering “teasers.” These teasers are generally free, sexually-explicit images. The web surfer is then offered similar images if they pay for access to the rest of the site.

Although publishing a website is somewhat more complicated than surfing the Web, any group or individual may publish a site on the World Wide Web. People are also generally free to publish sexually-explicit websites as well, subject to the administrative regulations of their internet provider. These sites are created, posted, and accessed in the same manner as sites that contain no sexual material. Individuals may receive webspace for the publication of a web page by paying a commercial provider. Webspace is also available for free through various providers like universities or companies such as Yahoo GeoCities, Xoom, and Angelfire which require webmasters to place the provider’s advertisements on any page published on its webspace.

Information available on the Web is often created, maintained, and controlled by one individual, and is located on separate computers found all over the world. At the time of the Reno II case, it was estimated that “60% of all content originates in the United States and 40% originates outside the United States.” The use of links on various web pages has created a very interconnected, though decentralized, environment on the Web. Indeed, a recent study suggests that any one, randomly-picked web page which features

64. Reno II, 31 F. Supp. 2d at 483.
65. Id. Navigating the Web via links is physically accomplished through using a computer mouse to direct an onscreen pointer and then by the user “clicking” the mouse button in order to follow that link to the next site. Reno I, 521 U.S. at 852.
67. Reno II, 31 F. Supp. 2d at 487. “Traffic” refers to the number of visitors to a particular website within a certain time.
68. Id.
69. Id.
70. Id.
71. Reno I, 521 U.S. at 853. “No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web.” Id.
72. Id.
74. Reno I, 521 U.S. at 853.
75. Reno II, 31 F. Supp. 2d at 484.
links to other websites which, in turn, have their own links to yet more such websites, is only nineteen clicks of a mouse away from any other such site. Thus, theoretically, a child browsing a children's website which features links to other sites is only nineteen clicks of a mouse away from any particular adult site with links.

After information is published on the Web, the publisher, also called a "webmaster," has no way of preventing the information on that website from being viewed by a particular person or community. Thus, once published, a webmaster can reach a potentially worldwide audience. No effective way of determining the age or identity of those who are accessing the information yet exists because visitors to websites remain anonymous. In addition, web surfers are typically reluctant to give any personal information about themselves to the publishers of a site.

Technically, the Internet is a collection of interconnected computer networks based on a standard known as Transmission Control Protocol/Internet Protocol (TCP/IP). Computers which use this protocol make up what is known as "the Internet." An IP address is registered to a particular server and consists of a set of numbers. Web surfers can access a site by using this IP address. However, an "alias" is usually used instead of the actual numeric IP address. Until recently, the Internet has been governed by NSFnet Internet Network Information Center (InterNIC), a consortium involving the National Science Foundation (NSF) and a private company, Network Solutions, Inc. (NSI). NSI had principal authority to register IP aliases through what have become known as "domain names." The domain names are generally represented by a hierarchical format of server.organization.type, such as "www.msnbc.com."
In 1999, the assigning of domain names was opened to a group of entities operating under the authority of the Internet Corporation for Assigned Names and Numbers (ICANN). For this system to work, someone must maintain a list of valid IP addresses and their aliases. The addresses and aliases are entered into a series of domain name servers (DNS) which are updated regularly. If the domain name is on the list, then a web surfer will be able to type in the alias and find the corresponding page on the Web.

B. “BOUNDARIES” IN CYBERSPACE

After gaining a general knowledge of the Internet and the World Wide Web, the tenuous nature of the boundaries from website to website becomes apparent. In real space, geographical boundaries exist. When someone talks to a person in real space, the person’s identity, appearance, location, and approximate age are generally known and even hard to conceal in many cases. When people communicate in cyberspace, however, that knowledge of identity, appearance, location, and approximate age disappear. Hence, in real space, governments can create zones within communities in which either children or merchants of adult material are denied access. A clear example is a bar. Most taverns require that people entering be of a minimum age, often age twenty-one. Indeed, bars will often employ people to stand at the door for the specific duty of checking people’s identification and denying minors’ access.

In cyberspace, however, this type of age verification is much more difficult, if not impossible, because once material is published on the Web, it is available to any anonymous web surfer in any community. New technologies are in the works which might create reliable boundaries in cyberspace or a reliable way of identifying a web surfer’s age, but these technologies are still in their infancy. Without the help of such technology, “it will be virtually impossible to transfer real space zoning principles to cyberspace.”

89. Id.
90. Id. at 1081.
91. Id.
92. Id.
94. Id. at 1148.
95. Id. These technologies under development include gateway technology, ratings systems, and domain naming. Id.
96. Id.
III. COMMUNICATIONS DECENCY ACT (CDA)

A. DESCRIPTION OF CDA

The first attempt at regulation of children’s access to adult materials on the Internet was Title V of the Telecommunications Act of 1996 known as the “Communications Decency Act of 1996” (CDA).\(^\text{97}\) It contained two provisions which would later be challenged in the \textit{Reno I} case.\(^\text{98}\) The first provision\(^\text{99}\) prohibits the knowing transmission of obscene or indecent messages to any recipient under eighteen years of age.\(^\text{100}\) The second provision\(^\text{101}\) prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under eighteen years of age.\(^\text{102}\) The Act also provides affirmative defenses.\(^\text{103}\)

\(^{97}\) CDA, 47 U.S.C.A. § 223(a).
\(^{98}\) See \textit{Reno I}, 521 U.S. 844.
\(^{99}\) CDA, 47 U.S.C.A. § 223(a). It provides that:

Whoever in interstate or foreign communications... by means of a telecommunications device knowingly makes, creates, or solicits, and 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;... knowingly permits any telecommunications facility under his control to be used for any activity... with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

\(^{100}\) Id.
\(^{101}\) Id. at § 223(d). It provides:

Whoever in interstate or foreign communications knowingly uses an interactive computer service to send... to a specific person or persons under 18 years of age, or uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication;... knowingly permits any telecommunications facility under such person’s control to be used for an activity prohibited... with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

\(^{102}\) Id.
\(^{103}\) Id. at § 223(e)(5). It provides an affirmative defense for whoever has:... taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications,
B. RENO V. ACLU (RENO I)\textsuperscript{104}

Immediately after the President signed the CDA into law, twenty plaintiffs filed suit against U.S. Attorney General Janet Reno and the Department of Justice challenging the constitutionality of the two provisions.\textsuperscript{105} The Court held that the two portions of the CDA at issue were unconstitutional.\textsuperscript{106} First, the Court determined that the provisions were not merely time, manner, and place restrictions but rather content-based blanket restrictions.\textsuperscript{107} The Court also distinguished the Pacifica case by stating that, unlike broadcast radio, people had to take affirmative steps to access the Internet. As such, the Internet more resembled the telephone medium in the Sable case. Just as people had to take affirmative steps in dialing their phones to receive an indecent message, people had to take affirmative steps in connecting to the Internet by opening the web browser, and finding a site with indecent material on it.\textsuperscript{108} Finding no rationale for a lesser standard of review, the Court applied strict scrutiny to the review of these provisions.\textsuperscript{109}

Under strict scrutiny, the provisions must be narrowly tailored to accomplish a compelling government interest.\textsuperscript{110} The Court found that the government did have a compelling interest in protecting children, but found that the government did not meet its burden of showing that the provisions including any method which is feasible under available technology; or has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

\textit{Id.}

\textsuperscript{104} 521 U.S. 844.

\textsuperscript{105} \textit{Id.} at 861. The district court had entered a preliminary injunction against enforcement of both of the challenged provisions after determining that the provisions were overbroad and unconstitutionally vague, and that the affirmative defenses were not "technologically or economically feasible for most providers." \textit{Id.} at 861-62.

\textsuperscript{106} \textit{Id.} at 885. Justices O'Connor and Rehnquist dissented in part. They felt that the CDA should not be invalidated when applied to individuals who send an indecent communication knowing all recipients are minors, as would be the case with an e-mail sent to a known juvenile. \textit{Id.} at 897 (O'Connor, J., dissenting in part).

\textsuperscript{107} \textit{Id.} at 868.

\textsuperscript{108} \textit{Id.} at 866-70. The Court reasoned that the "Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial." \textit{Id.} at 854. The Court also noted that the order in Pacifica was not punitive in the way the criminal statute here was. Plus, the Court noted that radio had historically "received the most limited First Amendment protection, in large part because warnings could not adequately protect the listener from unexpected program content." \textit{Id.} at 867.

\textsuperscript{109} \textit{Id.} at 868.

\textsuperscript{110} \textit{Reno I}, 521 U.S. at 868.
were narrowly tailored to accomplish that interest. The provisions were not found to be narrowly tailored because the Court felt that the government failed to show why less restrictive alternatives would not be as effective as the CDA. In addition, the provisions could not be considered narrowly tailored because of their ineffectiveness in limiting children's access to adult sites because some minors would have access to credit cards and because foreign sites would remain unregulated.

The Court also found that the provisions were too vague to allow for criminal prosecution because the term "indecent" was not defined in the CDA. Further, the term could not be measured by contemporary community standards because of the global nature of the Internet. Additionally, the Court found the provisions to be overbroad because they may affect small web publishers who do not have access to the age-verification methods mentioned in the affirmative defense, yet only intend their pages to be viewed by adults. The Court stated that the affirmative defenses would not save the provisions because the defenses were not reliable means of verifying age, and because they would stifle the speech of smaller, non-commercial publishers. The Court determined that "existing technology did not include any effective method for a sender to prevent minors from obtaining access to his communications on the Internet without also denying access to adults."

The Court also sought to distinguish this case from the Ginsberg case. First, the statute in Ginsberg did not prohibit parents from allowing their children to view the material, whereas the provisions in the CDA would presumably still be in effect even if the parents had given the children permission to view the material on the Internet. Second, the statute in

111. Id. at 875. The Court explained that the government's interest in protecting children "does not justify an unnecessarily broad suppression of speech addressed to adults." Id.
112. Id. at 879.
113. See id. at 882.
114. Id. at 872-73. The Court felt that the vagueness derived from the lack of any definition for "indecent" and "patently offensive," and to how the terms related to each other. Id. The Court found that the vagueness of the provisions would also lead to a chilling effect on speech because the severity of a criminal sanction of up to two years in prison "may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images." Id. at 872.
115. See id. at 874-77. The Court found that "it would be prohibitively expensive for non-commercial - as well as some commercial - speakers who have Web sites to verify that their users are adults." Id. at 877.
117. Id. at 876.
118. Id. at 864-67.
119. Id. at 865.
Ginsberg applied only to commercial transactions, whereas the CDA did not.\textsuperscript{120} Third, the CDA provisions omit the "without serious literary, political, scientific, or artistic value" terminology.\textsuperscript{121} Finally, the New York statute in Ginsberg defined a minor as a person under the age of seventeen, whereas the CDA applied to all those under eighteen years of age.\textsuperscript{122}

The Court also distinguished the Renton case.\textsuperscript{123} The Court found that, unlike Renton, the provisions here were not designed to prevent the secondary effects of the indecent speech, such as increases in neighborhood crime rates and deteriorating property values, but rather the primary effects of viewing the indecent material.\textsuperscript{124} In addition, the Court found the incorporation of real life zoning laws in cyberspace to be inappropriate since cyberspace contained little or none of the geographic boundaries of real space.\textsuperscript{125} As a result, the U.S. Supreme Court held the two provisions of the CDA to be unconstitutional because of vagueness, overbreadth, and the fact that they were not narrowly tailored.\textsuperscript{126}

IV. CHILD ONLINE PROTECTION ACT (COPA)

A. DESCRIPTION OF COPA

In response to the constitutional problems associated with the CDA, Congress passed the Child Online Protection Act (COPA)\textsuperscript{127} in October 1998.\textsuperscript{128} Like the CDA, COPA is a criminal statute.\textsuperscript{129} COPA provides that:

(1). . . 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. (2). . . In addition. . . whoever

\textsuperscript{120} Id.
\textsuperscript{121} Id.
\textsuperscript{122} Reno I, 521 U.S. at 865-66.
\textsuperscript{123} Id. at 867-68.
\textsuperscript{124} Id.
\textsuperscript{125} Id.
\textsuperscript{126} Id. at 864-85. The Court declined the government's argument that the provisions should be saved, by construing them narrowly, because it felt that doing so would be tantamount to rewriting the law. Id. at 882-85.
\textsuperscript{128} Reno II, 31 F. Supp. 2d at 476-77.
\textsuperscript{129} See COPA, 47 U.S.C.A § 231.
intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. . . [E]ach day of violation shall constitute a separate violation. (3). . . In addition. . . whoever violates Paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. . . [E]ach day of violation shall constitute a separate violation.130

COPA specifically provides that “[a] person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.”131 It states:

The term “engaged in the business” means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person’s trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person’s sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.132

130. COPA, 47 U.S.C.A § 231. Congress defined “harmful to minors” as: . . . any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest; depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

Id. at § 231(e)(6).
131. Id. at § 231(e)(2)(a).
132. Id. at § 231(e)(2)(B).
A minor is defined under COPA as any person under seventeen years of age. COPA provides affirmative defenses to prosecution under the statute. It provides that:

It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors by requiring use of a credit card, debit account, adult access code, or adult personal identification number; by accepting a digital certificate that verifies age; or by any other reasonable measures that are feasible under available technology.

B. COMPARISON TO CDA

Unlike the CDA, COPA only regulates commercial webmasters of sexual materials deemed harmful to minors. COPA is also much more limited in its scope in that it only deals with the World Wide Web and does not regulate other areas of the Internet such as chat rooms and listserves. COPA gave greater attention to detail in defining what type of speech would fit into the regulated area than what appeared in the CDA. COPA also reduced the minimum age of those who may permissibly view the websites mentioned in the statute from eighteen to seventeen. The penalty for violation of COPA remained, however, essentially the same as that found in the CDA: heavy fines and imprisonment. The time of imprisonment, however, was reduced from two years to six months. Yet, COPA also plainly states that each day of the violation shall be considered a separate violation. Although COPA only regulates those who are involved in the Web for commercial purposes, its definition of "engaged in the business" is quite broad. It includes in its definition of "engaged in the business" those who have the "objective of earning a profit as a result of such activities;" however, "it is not necessary that the person make a profit or that the making or offering to make such

133. Id. at § 231(e)(7).
134. Id. at § 231(c).
136. Id.
140. COPA, 47 U.S.C.A. § 231(a)(2).
141. Zick, supra note 15, at 1175.
communications be the person's sole or principal business or source of income." As did the CDA, COPA contains affirmative defenses to prosecution under the statute. These affirmative defenses, of course, still allow the government to bring charges against a defendant, but would allow that defendant to escape conviction if the defenses are proven. COPA also differs from the CDA in that it permits parents to allow material deemed "harmful to minors" to be viewed by their children who are under the age of seventeen without liability.

C. ACLU V. RENO (RENO II)

Immediately after COPA was signed into law, the ACLU and various other plaintiffs sought injunctive relief against the enforcement of it, claiming that it violated the First Amendment to the Constitution. After the court determined that the plaintiffs had standing to bring the suit, the plaintiffs argued that COPA was unconstitutional on three grounds: 1) that it is facially invalid under the First Amendment for restricting speech that is constitutionally protected for adults; 2) that it is facially invalid for violating minors' First Amendment rights; and 3) that it is unconstitutionally vague and overbroad under the First and Fifth Amendments. The plaintiffs also argued that a less restrictive means to achieve the goal of denying the access of minors to materials that are harmful to them was the use of "blocking" or "filtering"
The plaintiffs further argued that the blocking software is also more effective than COPA because, unlike the statute, it will restrict minors’ access to foreign and non-profit sites. The defense argued that COPA was constitutional because it passes the strict scrutiny of First Amendment review.

The Plaintiffs’ motion for a preliminary injunction enjoining the enforcement of COPA was granted by the district court on February 1, 1999. Relying on the Reno I decision, the U.S. District Court for the Eastern District of Pennsylvania applied strict scrutiny to the analysis of COPA. The court looked to the burden placed upon speech. It found that “[a] statute is presumptively inconsistent with the First Amendment if it imposes a financial burden on speakers because of the content of their speech.” The plaintiffs presented evidence that the financial burden on smaller, commercial webmasters could be such that their expression of speech could be severely diminished. The evidence showed that the start-up cost of credit card or age-verification services ranges from a few hundred dollars to thousands of dollars. In the alternative, a webmaster could pay for the services of a third party to provide online management of the credit card verification, although

151. Id. at 492. These types of programs may be downloaded and installed on a user’s home computer at a price of approximately $40.00. They can be used to block access to an entire website or specific pages within a website. Examples of these types of programs are Surfwatch, NetNanny, and Cyberpatrol. Id.

152. Id. The blocking software option also has its own difficulties, however, in that it may block out some appropriate sites and that a computer-savvy child may be able to defeat the program. Id.

153. Id.

154. Zick, supra note 15, at 1150 n.21. The Department of Justice filed a notice of appeal from the district court’s preliminary injunction on April 2, 1999. Id.


156. Id. The court felt that even if the defendant could show that the implementation of a credit card or adult verification system would be affordable to the plaintiffs at bar, that would not be enough. The court ruled that the First Amendment requires looking at the burden that the statute places on the type of speech itself, not just the financial burden upon the plaintiffs. Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 115 (1991) cited in Reno II, 31 F. Supp. 2d at 493.

157. Reno II, 31 F. Supp. 2d at 488. A webmaster would have to complete several steps to place an age or credit card verification system, including: 1) “setting up a merchant account;” 2) “retaining the services of an authorized Internet-based credit card clearinghouse;” 3) “inserting common gateway interface, or CGI, scripts;” 4) “possibly rearranging the content on the Web site;” 5) “storing credit card numbers or passwords in a database;” and 6) “obtaining a secure server to transmit the credit card numbers.” Id.

158. Id. The webmaster may even have had to transfer to a different ISP if the server which they currently used did not support credit card verification or CGI scripts. A secure server which supports credit card verification may cost a few thousand dollars. Id.
the website would incur additional costs for this service. These third parties would verify the credit cards for the adult webmaster and issue the web surfer an identification number which would be stored in the third party’s database. This would allow access to the adult areas of the webmaster’s site upon the web surfer’s entering of the identification number. Evidence provided by plaintiffs suggested that COPA would reduce anonymity of web surfers and thus lead to a great reduction in the traffic to the websites by adult web surfers. The district court determined that given the economical disadvantages, adult webmasters may engage in self-censorship of constitutionally-protected speech. In addition, the court found that COPA may also affect the free expression of speech in other internet communications such as chat rooms located within the website and would thus burden speech in an area not even covered by COPA.

Having established the burden on speech created by COPA and that strict scrutiny should apply, the court went on to consider the plaintiffs’ likelihood of success in showing that COPA is not narrowly tailored to achieve a compelling government interest. Not surprisingly, the court found that the government has a compelling interest in the protection of minors from adult materials deemed to be “harmful to minors.” The court did not find that the statute was narrowly tailored, however, because it felt that other means of accomplishing the government’s interest were available which were less restrictive of constitutionally-protected freedom of speech and that these alternatives were as effective, if not more effective, than a criminal statute. The court found that blocking programs were available and were much less restrictive of adults’ freedom of speech. Although these blocking programs were not found to be completely effective in restricting children’s access, they appeared to be more effective than COPA because the software could restrict

159. Id.
160. Id. at 489.
161. Id. Adult Check is an example of such a third party. A webmaster can sign up with Adult Check for free and earn up to 50 to 60% commissions from web surfers that signed up for Adult Check from that webmaster’s site. Adult Check provides webmasters with a script free of charge which the webmaster can then place anywhere on her site that she wishes to block access to minors. A web surfer may obtain an Adult Check identification number for a small yearly fee which may be paid online with a credit card or through mail with a check and a copy of a driver’s license or passport. Id. at 489-490.
162. Id. at 491.
164. Id.
165. Id. at 492.
166. Id. at 495.
167. Id. at 497.
168. Id.
access to foreign sites as well as domestic ones.\textsuperscript{169} In addition, the effectiveness of COPA was questionable considering that minors may have access to a credit card.\textsuperscript{170}

The court determined that the \textit{language} of the statute was also not the least restrictive manner in which to achieve the goal of protecting children.\textsuperscript{171} For instance, limiting the prohibited forms of content to only pictures, images, or graphic image files, rather than \textquote{any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind,\textquote{ as stated in the statute, would have been a less restrictive way of effectively restricting minors' access to the \textquote{teasers} commonly found on adult commercial sites.\textsuperscript{172} The court asserted that the goals of COPA might have been equally accomplished with the imposition of a penalty less severe than criminal liability.\textsuperscript{173} Also, the court mentioned that COPA may be less restrictive of constitutional rights if the elements in the affirmative defenses were instead made necessary elements of the prosecution.\textsuperscript{174} In sum, the court found that the plaintiffs had a likelihood of success in a trial on the merits of showing that COPA was not narrowly tailored in that it was not the least restrictive means available of achieving the goal of protecting children.\textsuperscript{175}

\textbf{D. ACLU V. RENO (RENO III)\textsuperscript{176}}

The decision of the district court in \textit{Reno II} was appealed by the Attorney General and oral arguments were heard on November 4, 1999.\textsuperscript{177} The Third Circuit affirmed the decision of the district court and upheld the granting of a preliminary injunction to prevent the enforcement of COPA. After determining that the district court had properly found that the plaintiffs had established standing, the circuit court began its analysis.\textsuperscript{178} The circuit court agreed with the district court that COPA was a content-based restriction on

\begin{itemize}
\item 169. \textit{Reno II}, 31 F. Supp. 2d at 497.
\item 170. \textit{Id.} at 496-97.
\item 171. \textit{Id.} at 497.
\item 172. \textit{Id.}.
\item 173. \textit{Id.}.
\item 174. \textit{Id.}.
\item 175. \textit{Reno II}, 31 F. Supp 2d at 498.
\item 176. 217 F.3d 162. The new United States Attorney General, John Ashcroft, filed a petition for writ of certiorari to review the decision in \textit{Reno III} and the U.S. Supreme Court granted that petition on May 21, 2001. \textit{Ashcroft}, 2001 U.S. LEXIS 3820, at *1. The U.S. Supreme Court will likely review the \textit{Reno III} decision sometime during the term which starts in October of 2001.
\item 177. \textit{Reno III}, 217 F.3d at 162.
\item 178. \textit{Id.} at 171-72.
\end{itemize}
speech and, as such, strict scrutiny should apply.179 The circuit court agreed that the government had a compelling interest in protecting children from harmful materials such as pornography.180

The circuit court affirmed the decision of the district court, but on much narrower grounds.181 The circuit court only addressed the issue of overbreadth.182 The court found COPA's definition of "harmful to minors" and its application of "contemporary community standards" to be unconstitutionally overbroad.183 The court found this overbreadth so concerning as to alleviate the need for reviewing any of the other provisions of COPA.184 The court based its entire opinion on this overbreadth and ignored the other grounds relied on by the district court.185 The court felt that the same "community standards" overbreadth problems found in the CDA remain in COPA.186 The court held that determining community standards on the Web was impossible because: 1) of the global nature of the Internet; 2) once material is placed on the Web, it is available to everyone unless password or credit card protected; 3) no reliable age-verification system exists; 4) the Web has no geographic boundaries; and 5) current technology does not allow webmasters to prevent

---

179. Id. at 173.
180. Id.
181. Id.
182. Id. at 173-74.
184. Id. at 174. The court felt that "this aspect of COPA, without reference to its other provisions, must lead inexorably to a holding of a likelihood of unconstitutionality of the entire COPA statute." Id.
185. Id. at 174 n.19. The court stated: 
...we do not find it necessary to address the District Court's analysis of the definition of "commercial purposes"; whether the breadth of the forms of content covered by COPA could have been more narrowly tailored; whether the affirmative defenses impose too great a burden on Web publishers or whether those affirmative defenses should have been included as elements of the crime itself; whether COPA's inclusion of criminal as well as civil penalties was excessive; whether COPA is designed to include communications made in chat rooms, discussion groups and links to other Web sites; whether the government is entitled to so restrict communications when children will continue to be able to access foreign Web sites and other sources of material that is harmful to them; what taken "as a whole" should mean in the context of the Web and the Internet; or whether the statute's failure to distinguish between material that is harmful to a six year old versus a sixteen year old is problematic.

Id.

186. Id. at 174. The court stated: "We are not persuaded that the Supreme Court's concern with respect to the "community standards" criterion has been sufficiently remedied by Congress in COPA." Id.
their material from being viewed by specific geographic locations with differing community standards.\textsuperscript{187} This fact means that a webmaster would need to apply the most restrictive community's standards in order to avoid criminal liability.\textsuperscript{188} Thus, minors would be prevented from accessing materials even if not deemed harmful to them in their particular geographic community, making COPA overly broad in its application.\textsuperscript{189}

The government argued that subjecting webmasters to varying community standards has been upheld in other cases, depending on the community in which the conduct took place.\textsuperscript{190} The court held that those cases are distinguishable because, unlike the Web, there existed an ability to control the distribution of the indecent material into different geographic locations.\textsuperscript{191} Defendants could thus avoid liability by avoiding those geographic locations with stricter community standards.\textsuperscript{192} Webmasters, on the other hand, currently have no way of controlling which geographic locations view their published materials, thus forcing the webmaster to either apply the most strict community standard or forgo publication altogether.\textsuperscript{193}

To elaborate on the court's reasoning, COPA uses community standards to determine what is "harmful to minors," but fails to define the relevant community that will set the standard.\textsuperscript{194} Given the global nature of the Internet and the fact that once a page is published on the Net, the publisher has no way to keep it out of a particular community, trying to determine a relevant community standard seems illogical. If a minor views sexual material in a sexually-conservative community on a web page that was published in a sexually-liberal community, which community standard should apply?\textsuperscript{195} Because publishers cannot predict what community standards will be used to

\begin{footnotesize}
\begin{enumerate}
\item[187.] Id. at 175.
\item[188.] Id.
\item[189.] Reno \textit{III}, 217 F.3d at 176.
\item[190.] Id. at 175. (Such as the "dial-a-pom" in the \textit{Sable} case).
\item[191.] Id. at 175-76.
\item[192.] Id. at 176. The court also distinguished United States v. Thomas, 74 F.3d 701 (6th Cir. 1996), in which the Sixth Circuit applied differing community standards in determining material placed on an electronic bulletin board to be harmful to minors, even if the material was acceptable in the community from which it was sent. Yet, access to the electronic bulletin board was available online only to members with passwords, and the geographic locations of these members could be determined before the passwords were issued. The defendants in that case could have thus refused to issue passwords to members in less tolerant communities. \textit{Id.}
\item[193.] Id.
\item[194.] Zick, \textit{supra} note 15, at 1194.
\item[195.] Some have suggested using an "internet community standard." \textit{See} Doherty, \textit{supra} note 15, at 288. Problems still arise, however, because the Internet community is so varied that it doesn't share a standard like geographic communities might. \textit{Id.}
\end{enumerate}
\end{footnotesize}
determine what is "harmful to minors," webmasters will be unable to predict what will and what will not be considered "harmful to minors." 196

The court stated that before they would invalidate a statute because of overbreadth they must first determine if it can be limited so as to cure the overbreadth by narrowing the meaning to the language of the statute itself or by deleting the portion of the statute that is unconstitutional. 197 The court refused to accept the government's suggestion that the statute be interpreted narrowly by construing the "contemporary community standards" language in COPA as an "adult" rather than as a "geographic" standard. 198 The court refused because it found no evidence that "adults everywhere in America would share the same standards for determining what is harmful to minors." 199 The court also refused to strike the overbroad "contemporary community standards" language from COPA because the standard is "an integral part of the statute, permeating and influencing the whole of the statute." 200 The court also refused to deny application of the overbreadth doctrine because of the commercial nature of COPA, because even though the Supreme Court has refused to apply the doctrine to statutes regulating commercial advertising, COPA regulated more than just commercial advertising. 201

While stating its inapplicability at present to the World Wide Web, the court was careful in stating that the holding does not diminish the application of Miller's "contemporary community standards" test. 202 The court also said that even though the district court focused on "the availability, virtues and effectiveness of voluntary blocking or filtering software that can enable parents to limit the harmful material to which their children may otherwise be exposed, the parental hand should not be looked to as a substitute for a congressional mandate." 203 Thus, the court leaves open the possibility of laws like COPA being constitutional if reliable geographic and age-verification technology is invented. The court stated its "firm conviction that developing

196. Id. at 289.
198. Reno III, 217 F.3d at 178.
199. Id. "To the contrary, it is significant to us that throughout case law, community standards have always been interpreted as a geographic standard without uniformity." American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 182-83 (S.D.N.Y. 1997), cited in Reno III, 217 F.3d at 178.
200. Reno III, 217 F.3d at 179. "We see no means by which to excise those 'unconstitutional' elements of the statute from those that are constitutional..." Id.
201. Id. at 179 n.22.
202. Id. at 180. "We remain satisfied that Miller's 'community standards' test continues to be a useful and viable tool in contexts other than the Internet and the Web under present technology." Id.
203. Id. at 181 n.24.
technology will soon render the "community standards" challenge moot, thereby making congressional regulation to protect minors from harmful material on the Web constitutionally practicable."

V. ANALYSIS OF COPA-LIKE LAWS

The Reno III case left open the possibility of a law like COPA being constitutionally sound if technology advances to the point where webmasters can reliably determine the web surfers' ages and approximate geographic locations. In such a case, the overbreadth problems which caused COPA to be held unconstitutional in Reno III would disappear. The next question becomes: Would a law like COPA be constitutional if such technology existed? The Reno II case would suggest otherwise. This comment will now analyze whether a law like COPA would withstand First Amendment scrutiny if such technology existed.

A. COPA UNDER RELIABLE GEOGRAPHIC AND AGE-VERIFICATION TECHNOLOGY

Based on the precedent of the Reno I case, any appellate court reviewing a law like COPA will likely apply a strict scrutiny standard. A law like COPA is a content-based restriction upon speech, and as such, will be viewed by the courts as presumptively invalid. Under the strict scrutiny analysis, the courts will undoubtedly find that the government has a compelling interest in protecting minors. What remains in doubt, however, is whether the courts will find such a criminal law to be narrowly tailored to achieve that goal.

Assuming that technology advances to the point where webmasters can reliably determine the age and approximate geographic location of the visitors to their sites, the government will make many arguments about how a law like COPA should be found to be narrowly tailored. The government is likely to argue that a law like COPA meets the concerns mentioned in the Reno I case. First, they will likely argue that COPA is limited to the effects of adult, commercial websites, thus avoiding the problems that the CDA faced relating

204. Id. at 181.
207. Jacobson, supra note 12, at 437. The "[s]tate's interest in safeguarding the physical and psychological well-being of a minor is compelling." Ferber, 458 U.S. at 757, quoted in Zick, supra note 15, at 1166-67. "The Court has stated that this interest extends to shielding minors from the influence of literature that is not obscene by adult standards." Sable, 492 U.S. at 126, quoted in Jacobson, supra note 12, at 437.
to sites maintained by private individuals on nonprofit websites.\textsuperscript{208} Second, the
government will point to the affirmative defenses in arguing that webmasters
will be protected from liability if they have made a good faith attempt to
restrict minors’ access to indecent materials. Third, the vagueness problems
of CDA were addressed in COPA by a more concrete definition of the term
“harmful to minors.”\textsuperscript{209} Fourth, the government can also assert that COPA,
unlike the CDA, preserves parents’ rights in allowing their children to view
such material.\textsuperscript{210} Finally, the government may also assert its right to regulate
the Internet based on the precedent of various internet intellectual property
laws already passed and upheld.\textsuperscript{211}

The plaintiffs will counter these arguments. First, they will point to the
broad definition of “engaged in the business” found within COPA. COPA
does not require the website to make a profit or for it to be the webmaster’s
principal business.\textsuperscript{212} This definition of “engaged in the business” is
problematic because many webmasters attempt to make a profit in ways other
than by selling access to adult material.\textsuperscript{213} For example, they may offer all
material for free, but attempt to make a profit through advertisements on their
website.\textsuperscript{214} A webmaster might also accept contributions from supporters while
leaving access to materials on the site free to visitors.\textsuperscript{215} Thus, these websites
would be considered commercial sites by the statute, but the webmasters may
have no desire to utilize age-verification technology on their site because
doing so would likely reduce the adult traffic to their site.

A law like COPA may place a considerable burden on free speech when
one considers the relative ease of webmasters to procure their own webspace
for sexually-explicit sites and to receive advertising for those websites.
Several free web servers exist which allow anyone with an internet connection
to build his own adult website free of charge.\textsuperscript{216} Several “partnership
programs” are available on the Web which offer “click-through” incentives
and commissions.\textsuperscript{217} These programs usually involve a webmaster placing a

\textsuperscript{208} Jacobson, supra note 12, at 439.
\textsuperscript{209} Id. at 438.
\textsuperscript{210} Id. at 441.
\textsuperscript{211} Id.
\textsuperscript{212} See COPA, 47 U.S.C.A. § 231(e)(2)(B).
\textsuperscript{213} See Reno II, 31 F. Supp. 2d at 486.
\textsuperscript{214} See id.
\textsuperscript{215} Cf. id.
\textsuperscript{216} See, e.g., \textit{Free Webhosting}, at http://www.xxxcity.net/freehost.html (last visited
Nov. 14, 1999) (listing several such free hosts of adult sites).
\textsuperscript{217} See, e.g., \textit{Partnership Programs}, at http://www.webmasterland.com/pages/
Money_programs_Partnerships.shtml (last visited Mar. 1, 2001) (listing several advertisers for
adult site webmasters).
"banner" on her site that links a web surfer to the partnership program provider. Thus, small websites which advertise in such a manner would be forced, under a law like COPA, to use an age-verification system even though their adult material itself is not commercial in nature. COPA would therefore be restricting a form of non-commercial speech. This type of overbreadth problem is similar to that which helped lead the Supreme Court to strike down the CDA.

Even the Justice Department found problems with COPA. It felt that COPA may divert resources away from "more important initiatives, such as combating online traffickers of hard-core child pornography and predators of children." The Justice Department also complained that there are ambiguities in the scope of COPA and that such ambiguities hinted that the statute may not be narrowly tailored to achieve the governmental interests. The Justice Department was also concerned over effectiveness of enforcement because "40% of web content originates overseas and cannot be regulated by United States law."

B. OTHER EARLY LANDMARK CASES

Some cases decided in federal courts across the country after the Reno I decision may provide some insight into the current state of law in this area and how courts will handle COPA-like laws.

1. Cyberspace v. Engle

A Michigan state law made it a criminal offense to disseminate sexually explicit materials to minors via computer. Plaintiffs challenged the

218. See id. The click-through incentives are usually three to five cents for every web surfer who clicks on the banner and a commission for every one of those web surfers coming from the webmaster's site that purchases something from the partnership program provider.
221. Id.
222. Id. The Justice Department was especially troubled by the ambiguities that arise as to which "contemporary community standard" would be dispositive. Id.
223. Id.
226. Cyberspace, 55 F. Supp. 2d at 740. Violation of the statute is a felony punishable by up to two years in prison and a fine of $10,000. Criminal sanctions could be applied if the sexually explicit material originated, terminated, or both originated and terminated in the State of Michigan. Id.
statute on grounds that it violated the First Amendment and the Commerce Clause of the U.S. Constitution.\textsuperscript{227} Under the court’s Commerce Clause analysis, the court determined that most web addresses for pages on servers within the United States contain no geographic indicators.\textsuperscript{228} The court ruled that the Internet is an instrument of interstate commerce.\textsuperscript{229} The court also determined that information on the Internet cannot be stopped at the Michigan border.\textsuperscript{230} The court ruled that the statute violated the Commerce Clause because it: 1) attempted to regulate activities that may occur entirely outside of the state; 2) created an unreasonable burden on interstate commerce; and 3) subjected internet users to inconsistent state regulations.\textsuperscript{231}

Applying strict scrutiny to the Michigan statute under First Amendment analysis, the court found that the state had a compelling interest in sheltering children from sexually explicit material, but found that the state failed to show that the statute was narrowly tailored to effectuate that interest because less restrictive means were available, namely, blocking software.\textsuperscript{232} The court also decided that the statute was unconstitutionally overbroad because it would restrict the speech of adults as well as minors.\textsuperscript{233} These findings by the court

\begin{footnotesize}
\begin{enumerate}
\item 227. See \textit{id}. The power granted to the U.S. government to regulate interstate commerce is also seen as a limitation over state governments’ ability to regulate it. This limitation over state governments’ power to regulate interstate commerce is known as the "Dormant Commerce Clause." Quill Corp. v. North Dakota, 504 U.S. 298 (1992).
\item 228. \textit{Cyberspace}, 55 F. Supp. 2d at 744. Many websites outside of the U.S. have indicators as to the country of origin within the domain name. For example, in "www.nic.ad.jp," the ".jp" designates a Japanese website. The Internet Assigned Numbers Authority (IANA) has a list of these country indicators. See \textit{IANA Root-Zone Whois Index by TLD Code}, at http://www.iana.org/cctd/ccitld-whois.htm (last visited Jan. 10, 2001). "TLD" stands for "Top Level Domain" and refers to designations such as ".jp" or "com" in the domain name. LEMLEY, supra note 81, at 1081.
\item 230. \textit{Cyberspace}, 55 F. Supp. 2d at 745.
\item 231. \textit{Cyberspace}, 55 F. Supp. 2d at 753-54. \textit{But see People v. Hsu}, 99 Cal. Rptr. 2d 184 (Cal. App. 1st Dist. 2000). The court found a California state law which prohibited the distribution of harmful matter to a minor over the internet did not violate the Dormant Commerce Clause. \textit{Hsu}, however, dealt with an instant message sent to a specific, known minor, rather than merely making the material available on a website. \textit{id}.
\item 233. \textit{id} at 747.
\end{enumerate}
\end{footnotesize}
led it to grant the plaintiffs’ motion for a preliminary injunction pending final
determination of these issues.234

2. ACLU v. Johnson235

A New Mexico statute236 criminalized the knowing dissemination by
computer of material that is “harmful to minors.”237 The court concluded that
the state failed to meet its burden under First Amendment strict scrutiny. The
state did not show that the statute was narrowly tailored to effectuate the
compelling state interest of protecting children.238 The court reasoned that
without the presence of a reliable age-verification system, any attempt at
enforcement of the statute would lead to ineffective results in that children
would still be able to access adult sites if they had access to a credit card.239
In addition, the statute would stifle the speech of adults because without a
reliable age-verification system it would be impossible for any webmaster to
place any material that might be deemed harmful to minors on the Internet
without “knowing” that the material could be accessed by a minor, thus
making them criminally liable merely for publishing the material itself.240
Additionally, the court determined that the statute violated the Commerce
Clause for the same reasons elaborated by the Cyberspace Court.241

3. Mainstream Loudoun v. Board of Trustees of the Loudoun County
Library242

Plaintiffs in this case claimed that their access to websites was
unconstitutionally blocked by the defendant library board’s policy.243 The
library’s policy was to block all material on the Web that it deemed harmful
to juveniles with web blocking software.244 The defendant library argued that
it had the absolute right to limit what it provides to the public.245 The court

234. Id. at 754.
235. 194 F.3d 1149 (10th Cir. 1999).
236. N.M. STAT. ANN. § 30-37-3.2(a) (Michie 1998).
237. Johnson, 194 F.3d at 1152. Defendants appealed from a grant of a preliminary
injunction enjoining the enforcement of the statute. Id.
238. Id. at 1159.
239. Id.
240. Id.
241. Id. at 161-64.
243. Id. at 556.
244. Id. A library patron could make a written request to the librarian to unblock a site
if she submitted her name and the reason she wanted the site unblocked.
245. Id.
found that while the library is not required to give its patrons access to the Internet, if it chooses to do so, it has limited ability to restrict access to it under the First Amendment. The court ruled that since the policy sought to limit the receipt of information on the basis of its content, the policy was subject to strict scrutiny under First Amendment review. The defendant claimed that the policy was the least restrictive method of securing the compelling government interests of: “1) minimizing access to illegal pornography; and 2) avoidance of creation of a sexually hostile environment ...” Because the defendant could provide little or no evidence that the policy minimized illegal pornography or reduced the occurrence of a sexually hostile environment, the court found that the library had failed to meet its burden of showing that the policy was reasonably necessary to further the accomplishment of the stated government interests. In addition, the court found that the policy was not narrowly tailored because of the existence of less restrictive alternatives like privacy screens or limiting the blocking software to only a few computers. The court also found the policy overinclusive because it limited the access not just of minors, but of adult patrons as well. The court further ruled that because the library’s ability to censor was virtually unbounded, and because no opportunity for review of a decision not to unblock a website was available, the policy constituted an unconstitutional prior restraint on free speech.

4. Urofsky v. Gilmore

Plaintiffs here challenged the constitutionality of a Virginia law restricting state employees from accessing sexually explicit material on computers that are owned or leased by the state. The court found that the

246. Id. at 562.
247. Id. at 563.
249. Id. at 566.
250. Id. at 567.
251. Id.
252. Id. at 568. Unconstitutional prior restraint of speech occurs “whenever the government makes the enjoyment of protected speech contingent upon obtaining permission from government officials to engage in its exercise under circumstances that permits government officials unfettered discretion to grant or deny the permission.” Baltimore Boulevard, Inc. v. Prince George’s County, 58 F.3d 988, 996 (4th Cir. 1995), quoted in Mainstream Loudoun, 24 F. Supp. 2d at 568.
253. 167 F.3d 191 (4th Cir. 1999).
255. Urofsky, 167 F.3d at 194. Under the law, a state agency head could give permission for a state employee to access sexually explicit material if the agency head deemed such access to be required in connection with a bona fide research project.
law did not regulate the speech of private citizens, but rather the speech of state employees in their capacity as such employees. Since the speech restriction only affected the employees in performance of their duties, the court ruled that the employer had a right to determine how those duties are performed. Because the law did not touch upon a matter of public concern, it did not violate the First Amendment. Although this case did not deal specifically with minors, it provided an example of a restriction on sexually explicit material over the Internet that was held constitutional.

C. RULE OF LAW

These four early landmark cases help shed some light on the burgeoning area of law relating to the restriction of children's access to adult sites on the Web. Although the small number of cases in this area makes determining a trend difficult, we can find some common threads. First, any state law attempting to regulate children's access to the Internet may encounter Commerce Clause problems. As the Cyberspace and Johnson cases make clear, the Web has thus far been viewed as a carrier of interstate and international commerce. Although the Virginia law in Urofsky was upheld, it was not challenged on Commerce Clause grounds. The Cyberspace and Johnson cases would at least suggest that any regulation in this area will have to be a result of federal rather than state legislation. Turning to First Amendment issues, internet regulations similar to that of COPA will be reviewed under strict scrutiny. This fact poses quite a challenge to lawmakers in that such regulations will be viewed as presumptively invalid unless it can be shown that no effective, less restrictive alternative is available.

D. FUTURE TRENDS

Three views will now be explored about the future of the law relating to the restriction of adult materials from children on the World Wide Web. The first is one espoused by Vickie Byrd in her note in the Howard Law Journal.

256. Id. at 196.
257. Id.
258. Id.
259. See Johnson, 194 F.3d 1149; see also Cyberspace, 55 F. Supp. 2d 737.
260. See, e.g., Johnson, 194 F.3d 1149; see also, e.g., Cyberspace, 55 F. Supp. 2d 737.
She argues that the decision of *Reno I* should be overruled. The second view is that expressed by Debra Keiser in her article in Albany Law Review stating that the decision in *Reno I* should be preserved, but the analysis should be altered. The final view is that of Timothy Zick, asserted in his article in the Creighton Law Review that the *Reno I* decision and analysis were correct and that as such, laws like COPA should be struck down as unconstitutional under the First Amendment. This comment will rebut the arguments of Byrd and Keiser and defend the arguments of Zick by asserting that they are the ones in accordance with the First Amendment case precedent.

1. Byrd's View

Byrd's note asserts the proposition that the *Reno I* case was decided incorrectly and the Supreme Court unconstitutionally usurped congressional authority. Byrd contends that the logic employed by the U.S. Supreme Court in *Reno I* was problematic because technology, rather than constitutional principles, drove the decision. Byrd’s first main contention is that the *Reno I* Court improperly distinguished the Internet from the broadcast medium in the *Pacifica* case. In *Reno I*, the Court did not lower the standard of review because, unlike broadcast radio in *Pacifica*, the Internet: 1) did not have a history of extensive government regulation; 2) was more similar to the telephone medium in *Sable*, and like the phone required affirmative steps on the part of the user to receive the indecent message since it was not “pervasive” like radio broadcasts; and 3) did not suffer from the “scarcity” problem of the radio.

Byrd argues that the Internet is more similar to broadcast radio than the *Reno I* Court believed because the Internet is a “fairly new medium” and “has not had a history of extensive government regulation like that of broadcasting.” This argument is odd considering that it is exactly what the Court in *Reno I* was saying: that there has been no history of extensive regulation in the Internet so as to provide a clear mandate of congressional authority to regulate it. But even assuming that Congress does have the

---

263. See id.
266. See Byrd, *supra* note 262.
267. See id.
268. Id. at 375.
269. See *Reno I*, 521 U.S. at 866-71.
authority to extensively regulate the Internet, the regulation at issue in the
Pacifica case was fundamentally different in that it was not a criminal statute,
but rather a FCC regulation. Moreover, one of the major issues of the case
was not just that the "filthy words" were broadcast, but that they were
broadcast at two o’clock in the afternoon when children were likely to be part
of the listening audience. Thus, while the regulation may have stifled
expression of indecent material during the day, the broadcasters were still
presumably left with the opportunity of expressing themselves at a later hour.

Byrd argues that the Court’s depiction of “a series of affirmative steps”
was incorrect because “[t]oday, ‘with just a few clicks’ of the mouse, a child
can summon pornographic and indecent images that would rattle the
sensitivities of an adult surfing the web.” Yet, even assuming that assertion
is true, it does not change the fact that the Reno I case more closely resembles
the Sable case. Children can simply pick up a phone and dial the number,
probably even more easily than they could visit a pornographic site on the
Internet. Neither the Internet nor the telephone is pervasive to the extent that
the radio is. A person may turn a radio dial with no forewarning about the
content of the next station. However, a child would mostly likely need some
sort of intent to hear or see the pornographic communication by dialing a
phone number or by finding the adult site.

Byrd next argues that since the “technology which drives computer
networks is controlled by a very small number of people, one can argue that
computer technology, in general, is also plagued by the ‘scarcity’ problem that
justifies limited First Amendment protection of broadcast communications.”
Yet, the technology driving the Internet is not the scarcity to which the Court
was referring. For instance, even if we assume that technology is controlled
by a very small number of people, such as Bill Gates for example, the current
availability of people to use that technology is almost limitless. Millions of
people all over the world have used that technology to create their own
websites, and it is those vast numbers of web publishers, not the scarce number
of computer engineers, that make the Web anything but scarce.

272. See Pacifica, 438 U.S. 726.
273. See id.
274. Byrd, supra note 262, at 375.
276. See id.
277. Byrd, supra note 262, at 375-76. “Scarcity” is discussed supra note 33 and
accompanying text.
278. See Reno I, 521 U.S. at 870.
279. See id.
280. Id.
Byrd then maintains that the Reno I Court’s determination of the vagueness and overbreadth of the CDA provisions was in error. Byrd argues that the meaning of “indecent” and “patently offensive” was not vague because “Congress made its intent and understanding apparent in the Conference Report on the CDA by stating that the term indecency [sic] as it appeared in the act was to have the same meaning as established in Pacifica and Sable.”

Yet, that legislative history does not change the fact that Congress failed to incorporate that, or any other, definition into the statute itself.

Byrd additionally argues that in the Denver Area Educational Telecommunications Consortium case, the United States Supreme Court “unequivocally rejected a vagueness challenge... [when] the provision at issue, which allowed cable system operators to prohibit the broadcast of indecent and obscene programming, used language similar to that adopted by the Supreme Court in Miller v. California [sic].... [and] was deemed to be ‘consistent with the First Amendment.’” First, the provisions at issue in the Denver Area Educational and Telecommunication Consortium case specifically defined terms in a manner similar to the Miller case, whereas the CDA failed to define its terms. Second, cable television is closer to the broadcast radio medium found in Pacifica than it is to the telephone or internet medium.

Byrd then asserts that the Court in Reno I was incorrect in finding that the CDA was overbroad. She states that “[t]he CDA was not a total ban on indecency; it only criminalized... the knowing display of indecent material to minors. Hence, under the CDA, adults would still have had access to indecent materials on the Internet.” The Supreme Court was not saying, however, that the CDA was unconstitutionally overbroad on its face, but rather overbroad in its application. Because no reliable age-verification system is currently available and because of the number of children currently using the Internet, it would be impossible for a webmaster to publish any adult material without “knowing” that it could be viewed by a minor. Thus, in order to avoid possible prosecution under the statute, the webmaster would have to avoid publishing the page altogether, which is exactly how the CDA could have
stifled free expression.

Byrd next contends that the CDA was the least restrictive means of achieving the compelling government interest of protecting children. She argues that “in order for alternatives to render an existing act unconstitutional, they must be as effective as the challenged law.” She states: “The alternative to the CDA, parental ‘self-help’ software, is seriously restricted in its efficacy.” It is true that the efficacy of software blocking programs is restricted; however, the CDA was too. Software blocking programs are at least as effective as, if not more effective than, the CDA, and do not restrict the freedom of expression of adults in the way the CDA would have.

2. Keiser’s View

In Keiser’s article, she argues that even though the Supreme Court’s final decision in the Reno I case was correct, she believes that the analysis was, to a certain extent, flawed. Keiser argues that the precedent of Renton should have played a bigger role in the Court’s decision: “What the Supreme Court ignores, and what Congress does not make clear, is that the CDA is not merely protecting children from viewing harmful material, it is also fighting crime.”

The Court in Renton upheld an ordinance regulating adult theaters, due to the secondary effects of those theaters, such as crime and deteriorating property values. The Reno I Court distinguished the Renton case by saying that the CDA was aimed at the primary effects of the indecent material on the Internet. Hence, the Court determined that the CDA should not be analyzed as a time, manner, and place restriction but rather as a content restriction, thus deserving of strict scrutiny.

Keiser argues that the purpose of statutes like the CDA is to contend with the primary effect of children being exposed to indecent material as well as the secondary effects of viewing that material. Keiser provides several examples that she describes as the crimes that are a secondary effect of the accessibility of adult material on the Internet, such as molesters and murderers

289. Byrd, supra note 262, at 381.
290. Id.
291. Id.
293. See Keiser, supra note 264.
294. Id. at 796.
295. See Renton, 475 U.S. 41.
296. Reno I, 521 U.S. at 867-68.
297. Id.
298. See Keiser, supra note 264, at 797.
luring children from chat rooms into their devious hands. Nonetheless, the CDA would likely not have kept these unfortunate children away from these chat rooms. Unless the topics of these chats would be considered "indecent" or "patently offensive," they would not have been covered by the CDA. These chats were likely innocent enough in and of themselves. The real indecency would not likely begin until the children were lured away from the chat room and into the real world of these offenders. Presumably, a molester could hunt for child victims in a "clean" chat room just as easily as he could in an "indecent" one. In addition, the Renton case dealt with a time, manner, and place restriction in that the zoning ordinance only prohibited an adult theater from being within 1,000 feet of a school, church, residence, or park. The adult theater owners could still express themselves outside of that 1,000 foot area. Under the CDA, however, many adult webmasters would be forced to forgo expressing themselves on the Internet altogether.

Next, Keiser argues that the underinclusiveness of the CDA, in its ineffectiveness against foreign webmasters, should not have been involved in the determination of the Reno I case. Keiser gives two arguments supporting her assertion. First, she contends that "most laws intended to protect children are not infallible. For example, laws exist which aim to prohibit minors from drinking alcohol. . . ." Second, Keiser argues that the mere "existence of laws and the consequences of breaking the laws influence crime rates." Yet, much to the chagrin of party animals everywhere, unlike speech, the Constitution does not give individuals a right to drink alcohol. Therefore, underage drinking laws are not subject to the same strict scrutiny of review as laws that restrict speech.

3. Zick’s View

In Zick’s article, he concludes that the Reno I and II cases were decided correctly. His contention is that the CDA and COPA would fundamentally alter the media of the Internet. Zick’s view is correct because if COPA were

299. See id.
300. See Renton, 475 U.S. 41.
301. See Reno I, 521 U.S. at 872.
302. See Keiser, supra note 264, at 798.
303. Id.
304. Id.
305. Id. at 799.
306. Although the Twenty-First Amendment to the U.S. Constitution repealed federal prohibition, it still permits state regulation of alcoholic beverages. U.S. CONST. amend. XXI.
308. Id. at 1195-96.
constitutio nal, thousands of internet users would be deterred from expressing themselves on the Internet.\footnote{309} Such a suppression of speech is even more undeserved considering that COPA would likely be ineffective in protecting children from indecent websites when children will still have access to all the sites that originate from outside the U.S.\footnote{310} In addition, many of the large, commercial, adult websites are likely to move to a server outside of the U.S. rather than removing or toning down “teasers” which are often highly effective in increasing traffic to their sites.\footnote{311} Considering that blocking programs, which can block out foreign websites, exist and do not create the problems of infringing on the rights of adults’ freedom of speech, laws like COPA will not likely be found to be the least restrictive means of accomplishing the goal of protecting children and thus will not pass the strict scrutiny required by the First Amendment.\footnote{312}

VI. ALTERNATIVE MEASURES

In order to survive strict scrutiny, laws like COPA must be both effective and the least restrictive means among other effective alternatives.\footnote{313} Yet, several alternative means are available which would restrict minors’ access to adult material deemed harmful to them while not restricting adult First Amendment rights.\footnote{314} Future laws that support or complement, rather than compete with, these alternative means should be preferred. Means of restricting children’s access to adult materials can be divided into two categories: filtering and zoning.\footnote{315} Laws like the CDA and COPA were themselves a type of zoning solution to the problem of restricting children’s access to adult sites,\footnote{316} but alternative zoning techniques also exist and, along with filtering solutions, will be explored in this Part. Filtering has been an alternative pursued since the failure of the CDA to pass constitutional muster in \textit{Reno I}.\footnote{317} Filtering involves blocking adult sites.\footnote{318} Zoning focuses on segregation of adult sites from general-access sites.\footnote{319} This comment will now

\footnotesize{\begin{itemize}
\item \textit{See Reno I}, 521 U.S. at 872.
\item \textit{See Reno II}, 31 F. Supp. 2d at 496.
\item \textit{See id.} at 476.
\item \textit{See Zick, supra} note 15 at 1191-93.
\item \textit{Id.} at 1192.
\item \textit{See id.} at 1160-62.
\item \textit{Lawrence Lessig, Code and Other Laws of Cyberspace} 175-76 (1999).
\item \textit{Id.} at 176-77.
\item \textit{Lessig, supra} note 315, at 176.
\item \textit{Id.} at 175.
\end{itemize}}
review both methods in turn, including the strengths and weaknesses of each as alternatives to laws like COPA.

A. FILTERING

Filtering is generally considered a way for web surfers to block sites or pages on the Web which they find objectionable, either personally or to their children.\textsuperscript{320} Filtering can be used by individuals, Internet providers, or jurisdictions.\textsuperscript{321} Filtering can be accomplished through the use of either hardware or software.\textsuperscript{322} Due to the much greater ease of software blocking over hardware blocking, most people interested in filtering websites opt for software.\textsuperscript{323} Blocking software can either work solely within its own programmed parameters, or work in conjunction with content ratings.\textsuperscript{324} Software that relies solely on the parameters set forth by the user or software manufacturer is called "stand alone blocking software."\textsuperscript{325} A common type of blocking software that works in conjunction with outside content ratings is that found on all the latest versions of the Internet Explorer and Netscape web browsers.\textsuperscript{326}

I. Stand Alone Blocking Software

Stand alone blocking software does not use outside ratings but only the parameters for blocking set forth by the software manufacturer, the software user, or both.\textsuperscript{327} Filtering software can work by using either a "fixed" or "heuristic" system.\textsuperscript{328} Software using a fixed system can block entire hosts or specific pages on a given host.\textsuperscript{329} These hosts or pages are blocked using a fixed list of known objectionable web addresses.\textsuperscript{330} The software will block these sites or pages unless proper authorization, like a password, is supplied.
to remove the block.\textsuperscript{331} Due to the fact that the Internet is constantly growing and changing, blocking software which uses fixed lists often encounters two related problems: 1) being labor-intensive to the administrator of the list; and 2) failing to block newly formed or mirrored objectionable sites.\textsuperscript{332}

Other types of blocking software exist which do not rely on constantly updated lists.\textsuperscript{333} These programs filter heuristically by searching requested URLs for potentially objectionable material, and making educated guesses about whether the page would in fact be objectionable.\textsuperscript{334} They deny access to the site if the program determines a high probability of objectionable content.\textsuperscript{335} The educated guesses about the content of the site are based on keywords and metatag information on the site.\textsuperscript{336} This type of information garnished from the site is not always an accurate proxy for the content of the site.\textsuperscript{337} As such, heuristic blocking software will sometimes make inaccurate guesses about a site and either block a site with useful and non-threatening information, or not block a site with objectionable information.\textsuperscript{338}

Filtering programs also allow more parental control over the content that their children see because many such programs allow the parent to choose which adult sites they want to block out while allowing other types of adult sites to be viewed.\textsuperscript{339} In addition to sexually explicit sites, blocking programs can also filter out other sites that parents find questionable, such as hate sites and drug-related sites.\textsuperscript{340} Also, unlike COPA, blocking software will limit the access of children to non-commercial sites without running into the First Amendment difficulties found in the CDA.\textsuperscript{341}

\begin{itemize}
\item \textsuperscript{331} Id.
\item \textsuperscript{332} Id. at \textsuperscript{10}. A “mirror” is a duplicate of another site at a different web address.
\item \textsuperscript{333} Id. at \textsuperscript{11}.
\item \textsuperscript{334} Id.
\item \textsuperscript{335} Id.
\item \textsuperscript{336} Id. A “metatag” is a special HTML instruction embedded in the HTML code which provides web browsers with information about the web page, including information about what the page contains. Search engines often use these metatags in cataloging web pages. LEMLEY, \textit{supra} note 81, at 1095.
\item \textsuperscript{337} Furlow, \textit{supra} note 322, at \textsuperscript{11}.
\item \textsuperscript{339} Doherty, \textit{supra} note 15, at 295-96. Cyber Patrol uses fifteen categories including “violence/profanity” and “sexual acts” and assigns a label of “CyberNOT” or “CyberYES” within each category. CYBERsitter, on the other hand, blocks only a single set of questionable sites with no opportunity to block only a part of any list. \textit{Id}.
\item \textsuperscript{340} Zick, \textit{supra} note 15, at 1162.
\item \textsuperscript{341} Id. at 1193.
\end{itemize}
This kind of software runs into other difficulties when it rejects coded "dirty" words which appear in the text of a document. For example, "Scunthorpe, England" may be blocked because of the word "cunt" embedded within the city name. As filtering programs continue to improve, problems such as these are likely to start disappearing. Another problem with blocking programs that use keywords is that they are not going to be able to filter out sexually explicit pictures unaccompanied by text. Despite the problems with the blocking software, evidence suggests that it is a reasonably effective method of assisting parents' attempts to restrict their children's access to adult sites.

2. Content Ratings

Blocking software can also be used in conjunction with outside ratings. Assuming the sites were rated accurately, the blocking software would be able to block sites much more effectively since fixed lists would not need to be maintained and updated, and because decisions to block would be based on a predetermined rating rather than keywords and metatag information. Currently, the foundation for such a rating system appears to be a technology called "Platform for Internet Content Selection" (PICS). PICS is not a rating system, but rather a set of protocols which would allow webmasters or independent third parties to rate a site.

PICS is the system currently used by the Internet Content Rating Association (ICRA). The ICRA is an independent, international organization which offers ratings, using the PICS standard, to webmasters who complete ICRA’s online questionnaire about the content of their sites. The ICRA system can currently be used with the blocking software that comes standard in both Internet Explorer and Netscape Browsers. The ICRA questionnaire covers the topics of language, nudity and sexual content, violence, and a miscellaneous category covering gambling, drugs, and

346. Reno I, 521 U.S. at 877.
347. Dobeus, supra note 317, at 633.
348. Id. at 627.
349. Id.
350. About ICRA, supra note 326.
351. Id. The ICRA’s forerunner was the Recreational Software Advisory Council on the internet (RSACi), but they turned control of internet rating over to ICRA in April of 1999.
352. Id.
alcohol.\textsuperscript{353} Within each of these broad topics, the webmaster is asked 
questions about whether a specific item is present on his site.\textsuperscript{354} The 
questionnaire also asks if the material featured on the site is suitable for young 
children because it is intended to be artistic, educational, or medical in 
nature.\textsuperscript{355} The ICRA system is not without controversy though. Specifically, 
many people disagree with the PICS ratings.\textsuperscript{356} Indeed, any ratings standard 
is bound to be skewed by the personal, cultural, religious, and moral values of 
those who created it.\textsuperscript{357}

If legislation is passed which requires such ratings,\textsuperscript{358} and the webmaster 
disagrees with the rating system used, First Amendment issues may be raised 
as well.\textsuperscript{359} Can a webmaster be forced to associate with a ratings system with 
which she does not agree? In his article in the John Marshall Journal of 
Computer and Information Law, James V. Dobeus argues that webmasters 
could not be forced to do so under the First Amendment.\textsuperscript{360} He cites a series 
of cases dealing with a First Amendment right \textit{not} to speak or associate with 
speech.\textsuperscript{361} Mandatory rating laws may force webmasters to use a rating system 
with which they fundamentally disagree.\textsuperscript{362} The government would, in effect, 
be requiring webmasters to use speech, in the form of ratings, which they 
otherwise would not make if not under threat of liability.\textsuperscript{363} The webmaster's 
only other real option in such a circumstance would be to refrain from any 
speech at all on his website.\textsuperscript{364} Additionally, making ratings mandatory may

\begin{itemize}
\item \textsuperscript{353} Id.
\item \textsuperscript{354} Id.
\item \textsuperscript{355} Id.
\item \textsuperscript{356} Dobeus, supra note 317, at 628-29.
\item \textsuperscript{357} See id. at 646.
\item \textsuperscript{358} Such legislation has been proposed before. See id. at 629 n.18.
\item \textsuperscript{359} See id. at 650-53.
\item \textsuperscript{360} See id.
\item \textsuperscript{361} Id. The First Amendment not only guarantees a right to speak, but also a right not 
to speak (Citing Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 559 
(1985)). The Supreme Court has held that the government cannot force a person to speak where 
the person would otherwise remain silent (Citing Riley v. National Fed. of the Blind, Inc., 487 
U.S. 781 (1988)). The Supreme Court has also held that compelling the disclosure of names 
and address of election materials was unconstitutional even though the disclosures were factual 
and assisted voters (Citing McIntyre v. Ohio Election Comm., 514 U.S. 334 (1995)). The 
government cannot force someone to advocate an ideological point that the person finds 
unacceptable (Citing Wooley v. Maynard, 430 U.S. 705 (1977)). The Court has also ruled that 
a speaker has a right not to be forced to associate with statements the speaker would rather 
avoid (Citing Hurley v. Irish-American Gay, Lesbian and Bisexual Group, 515 U.S. 557, 573-74 
(1995)).
\item \textsuperscript{362} Dobeus, supra note 317, at 650.
\item \textsuperscript{363} Id.
\item \textsuperscript{364} Id.
\end{itemize}
force some webmasters to associate the ratings with their internet speech. Based on prior Supreme Court precedent, Dobeus argues, these facts would make such a mandatory ratings law unconstitutional.

Assuming websites are rated, either on a mandatory or voluntary basis, the ratings will most likely appear in one of two possible forms: tagging or restricted top-level domains (rTLD). An example of tagging legislation would be a requirement that all web publishers provide a label imbedded within either the HTML code or the web address of the site to include words like “xxx” or “adult.” A label within the HTML code would presumably be included in the metatag. A web address label, on the other hand, may read as follows: “www.site.com/adult/content.html” where “adult” would denote that the site contains adult material. Webmasters would thus be required to review their webpages before they published them on the Web and determine whether adult material appears on them. Blocking software would then become much more effective in filtering out adult sites because rather than searching for keywords, it could simply search for the adult label in the metatag or web address.

The current keyword search utilized by several blocking programs is less accurate. For example, a keyword filter may block a site about a recipe for chicken because it contains the word “breast.” This sort of self-labeling of one’s website would be similar to the current “Parental Advisory” stickers placed on music albums by record companies. Unlike albums, which primarily deal with explicit language, a useful internet tagging system would, of course, contain more categories than just “adult” and “child-suitable.” An alternative to self-labeling sites would be a requirement to register one’s websites with a third party. The third party then would make an independent determination of the tag to be placed in the HTML code or web address. Different ratings could then be administered by different organizations. This sort of labeling is similar to the MPAA rating system of motion pictures.

365. Id. at 652.
366. See id. at 650-54.
367. See Zick, supra note 15, at 1160-61; see also Furlow, supra note 322, at ¶ 4.
368. Zick, supra note 15, at 1161.
369. Id.
370. Id.
372. Id.
373. Id.
374. Id.
Restricted top-level Domains (rTLD) would also include labels such as "xxx" or "adult," but would be incorporated into the top-level domain name. The web address would thus look something like this: "www.site.adult" where the familiar "\.com" would be replaced with "\.adult." Restricted top-level domains "would require that judgments be made concerning whether the content of a site requires that it be located within the new domain and would further require that software be developed to block sites based upon the new domain names." A possible advantage to rTLD over tagging would be that it could be implemented by ICANN. Whether ICANN will be able to enforce webmaster compliance with rTLD is another matter altogether. One possible ICANN enforcement mechanism could be the revocation of the domain names for failing to comply with the zoning requirements.

B. ZONING

Both the CDA and COPA attempted to zone the Internet through threat of criminal prosecution. Two basic types of internet zoning are available, both of which attempt to certify a web surfer's age. One type tries to certify that the web surfer is an adult, "adult certification," and the other type tries to certify that the surfer is under eighteen years of age, "child certification." Both the CDA and COPA focused on adult certification. Adult certification denies access to everyone except those who certify themselves as adults. Child certification, on the other hand, would grant access to the site to everyone except those that certify themselves as children. Adult certification would place more of a burden on both web surfers and webmasters, but it would also provide greater protection to children.

375. Furlow, supra note 322, at ¶ 4. The rTLD type of rating is also referred to as "DNS Zoning." See Zick, supra note 15, at 1161.
376. Furlow, supra note 322, at ¶ 4.
377. Id.
379. Furlow, supra note 322, at ¶ 55. ICANN is the administrator of the DNS.
380. Id.
381. Id. at ¶ 58.
382. LESSIG, supra note 315, at 177.
383. Id. at 176.
384. Id.
385. Id. at 177.
386. Id. at 176.
387. Id. Child certification would rely on age-verification technology such as digital certificates.
388. Id. Child certification would be less of a burden on adult web surfers because they would not have to set up a digital certificate for themselves since the default decision is to allow entry. Child certification would be less of a burden on webmasters because they would only
COPA’s affirmative defense section sets out the various means of adult certification, including the use of credit cards, debit accounts, adult access codes, adult personal identification numbers, and digital certificates. As discussed earlier, credit and debit cards present a problem in that some minors may have access to them, and some adults may not. Age verification must be more precise in order for zoning to work.

Adult passwords are more precise than credit or debit cards, but they present a different problem. Age verification based on passwords could make surfing from one adult site to another difficult if password entry was always required. A solution to this dilemma would be the use of a “cookie.” A cookie in cyberspace refers not to a sweet, home-baked treat, but rather to a program placed in a “cookie file” on a surfer’s hard drive by the site being visited. After the site places the cookie, the site will be able to receive various information about the surfer. The advantage of cookies is that they offer seamless verification. In other words, unless the surfer sets the web browser to notify him of cookie exchanges, he can browse the Web with little or no interruption. The disadvantage of cookies is that some surfers view them as an invasion of privacy, since they can be used to gain all sorts of information about the surfer other than age.

Digital certificates, on the other hand, would provide the security of passwords and the convenience of cookies. A digital certificate would reside on the web surfer’s hard drive, and would provide information about the surfer, including the surfer’s age. When the surfer entered the site, the site would automatically check the certified information. The surfer could release only the information she wanted to only those she wanted. Parents concerned about what their children view on the Web could require that their children use a digital certificate which indicated the child’s birth date.

be liable for allowing entry of a surfer who had certified that he was a minor. Adult certification would provide greater protection in the sense that a child could not circumvent a parent’s wish to restrict access to adult sites by using a computer outside the home that did not contain a digital certificate.

390. Lessig, supra note 315, at 34.
391. Id.
392. Id.
393. Id.
394. Id. at 41-42. Enabling the cookie notifier is a defense against this invasion of privacy, but most surfers find the constant alerts of cookie exchanges too annoying to tolerate. Id.
395. Id. at 35. Digital certificates would rely on encryption technology in order to make them secure.
396. Id.
397. Id.
Computers could be set up to have a different digital certificate for each user of the home computer. Access to the Internet could be denied on the computer unless a digital certificate was activated first. The child would only have the password to activate the digital certificate with his or her information on it. Adult websites could be set up so as to allow entry only to those surfers who have a digital certification of adult status. Additionally, unlike zoning based on adult passwords or credit cards, digital certificates could differentiate between older and younger children's ages. A webmaster may thus compose a site which she feels is suitable for teenagers, but not for children under the age of thirteen. She may then deny access to younger children and allow access to teenagers.

Although much of the current focus is on filtering, noted cyberlaw scholar, Lawrence Lessig, contends that digital certificate zoning is a better alternative to filtering in that it is more accurate than stand alone blocking software and that it avoids the "upstream invisibility" problems of blocking software used in conjunction with content ratings. The problems of content ratings, Lessig argues, spring from the neutrality of the PICS format. Lessig warns that the filtering is not only "horizontally neutral," allowing the individual surfer to choose which types of sites to block, but also "vertically neutral," allowing the filtration to occur at any level of the distribution. Although most think of filtration occurring on the surfer's computer, Lessig points out that filtration can occur further up in the distribution chain. This "upstream filtering" can occur at the organization through which the surfer gains internet access, at the surfer's ISP, or even at the jurisdiction in which the surfer resides. Since filtration at a point further upstream than the surfer's computer could be completely invisible to the user, filtration could be done without the surfer even being aware of it.

With digital certificate zoning, however, the individual would know when she was being denied access. Thus, any unjustified exclusion could be challenged by the person being blocked. Digital certificate zoning would allow individuals to choose their own filters rather than potentially having the filters chosen for them. Yet, in order for digital certificate zoning to work,

---
398. See id. at 181.
399. Id. at 178.
400. Id.
401. Id. at 178-79.
402. Id. at 178.
403. Id. at 179.
404. Id.
405. Id.
406. Id.
the adult sites must have verification technology so that they can check the
digital certificate. Such verification technology is still costly, and if digital
certification of age is required, smaller, non-commercial, adult webmasters
might not be able to comply with this requirement. The cost of digital
certificate verification technology is similar to the concerns expressed by the
Reno I Court about the costs of credit card verification technology stifling the
speech of non-commercial, adult webmasters. A digital certificate zoning
law could limit itself to commercial websites, but lawmakers should be careful
to give a narrower definition than that of “engaged in the business” found in
COPA. COPA’s definition would have included many smaller web
publishers whose speech would have been stifled because of the financial
burden placed upon them.

C. FINDING THE APPROPRIATE ALTERNATIVE

Problems exist with both filtering and zoning solutions. Stand alone
blocking software is a powerful tool which avoids all the First Amendment
concerns faced by government legislation. Nonetheless, current technology
which uses fixed lists or heuristic search methods will not be completely
effective in blocking out harmful materials. Blocking software used in
conjunction with content ratings avoids the problems associated with fixed
lists and heuristic search methods, but it remains inadequate since most sites
on the net are still not rated for content. If a website is not rated, then PICS
compatible software will block it as “unrated.” Thus, many useful and non-
threatening sites will be filtered. A federal law requiring mandatory content
ratings will make this software more effective, but such a law may also violate
First Amendment rights of webmasters. Even if constitutional, we must
consider whether we would even want a filtering system that used ratings and
blocking software. The possibility of overfiltration and censorship becomes
more likely with a PICS rating system.

407. Furlow, supra note 322, at ¶ 50.
408. Id.
409. See Reno I, 521 U.S. at 856.
412. See Furlow, supra, note 322, at ¶ 9; see also Doherty, supra note 15, at 297.
413. Dobeus, supra note 317, at 650. PICS-based ratings systems only filter potentially
harmful material effectively if all unrated sites are blocked as well. Weinberg, supra note 338,
414. See Dobeus, supra note 317, at 650-54.
415. See LESSIG, supra note 315, at 178-79.
Zoning solutions provide an alternative to filtration. Adult certification zoning by threat of criminal prosecution is not the answer under current technology as the *Reno* cases made clear.\(^\text{416}\) Legislation that promotes the development of inexpensive and effective age-verification technology seems more appropriate. At present, digital certification zoning appears to be the best long term solution to the problem of children's access to harmful material on the Web. Yet, enforcement of a digital certificate zoning method must wait until verification technology becomes affordable and simple enough for all webmasters to use. At that time, a law requiring webmasters to utilize such verification technology will not encounter the problems of stifling the speech of smaller, non-commercial webmasters. Such inexpensive digital certificate verification technology does not currently exist however. Until such time as it does, stand alone blocking software is the best short term remedy to the problem of denying children access to adult material on the Web, while preserving the First Amendment rights of adults.

VII. CONCLUSION

In the *Reno I* case, the Supreme Court dealt with the freedom of speech as it relates to the restriction of adult material on the Internet for the first time. Like the technology that guides the Internet, the laws that seek to regulate it are in their infancy. While use of the Internet as a means of communication is growing at an incredible rate, it still remains a novel and often misunderstood medium by many. Early attempts by states to restrict minors access to the Internet have run into Commerce Clause problems.\(^\text{417}\) As a result, future legislation will likely come in the form of federal statutes. Any attempt to "conquer" the wilds of the new information superhighway in haste, without allowing for technological development, will likely result in the undue subjugation of adults' First Amendment rights.\(^\text{418}\) While making the Internet safe for children is an important concern, that safety cannot come at the expense of adults' freedoms. The Internet has the potential to open up a whole new world of free expression which will allow people to communicate new ideas to a group as diverse and numerous as anything known before in the history of humankind, but not, however, if the reins on this new technology are pulled in too tightly, too quickly.

---

\(^{416}\) See *Reno I*, 521 U.S. 844; *Reno II*, 31 F. Supp. 2d 473; *Reno III* 217 F.3d 162.  
\(^{418}\) See *Reno I*, 521 U.S. 844.
Much of the uncertainty that remains in this area of law will be cast aside as computer technology and Internet case precedent continues to develop. For the time being however, cases like Reno, Cyberspace, and Johnson suggest that laws like COPA will be tough to defend against the strict scrutiny of First Amendment review, especially when less restrictive alternatives like blocking software exist and continue to improve. Under the current state of internet law, perhaps Congress would be better served by showing restraint when it comes to criminal statutes regulating indecent material on the Web and instead focusing on encouraging advances in blocking software and age verification.

Until such time as age-verification technology improves and becomes affordable to all webmasters, stand alone blocking software is the best way of achieving the government's objective of protecting minors from indecency on the Web while preserving adults' rights. When age-verification technology does become widely available and affordable, digital certification zoning may then become the long-term solution.

TIM SPECHT