Traditional Free-Speech Law: Does It Apply on the Internet?

by
*A. John Harper III**

I. INTRODUCTION

The First Amendment states that Congress "shall make no law . . . abridging the freedom of speech, or of the press."[1] But as Oliver Wendell Holmes recognized, the First Amendment "obviously was not intended to give immunity for every possible use of language."[2] Accordingly, the Supreme Court's free-speech jurisprudence has traditionally been one of line drawing — distinguishing protected from unprotected speech by evaluating its content in light of the medium through which it is expressed. In terms of content, there are generally three categories of speech: "(1) speech that everyone has a right to (political speech, speech about public affairs); (2) speech that no one has a right to (obscene speech, child pornography); and (3) speech that some have a right to but others do not" (speech that adults have a right to but children do not).[3] In terms of the medium of expression, the First Amendment provides more protection for certain locations and certain types of mass media.

This article examines the issues involved in attempting to apply existing free-speech jurisprudence to speech on the Internet — a new kind of medium whose degree of constitutional protection has not yet been firmly established. Section II discusses the ways in which information is stored, transferred, and accessed on the Internet. Section III reviews the Supreme Court's doctrine delineating the various degrees of protection afforded different types of media and concludes that the Internet should receive the highest level of protection. This conclusion means that any content-based restriction on Internet speech must be necessary to serve a compelling state interest, must be narrowly tailored to achieve that end, and must be the least restrictive means of accomplishing the government's interest.

---

* Mr. Harper practices labor and employment law with Haynes and Boone, L.L.P., in Dallas, Texas.

1. U.S. CONST. amend. I.

2. Frohwerk v. United States, 249 U.S. 204, 206 (1919).

3. Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 395 (1999).

Section IV applies this test to Internet speech, considering statutes regulating pornography and indecent communications. In each case, the article concludes that the anonymity and geographic pervasiveness of the Internet make traditional analysis unsuitable.

Finally, the article examines possible solutions to the problems raised by the application of obscenity statutes and indecency rules, and their associated First Amendment protections, to web-based speech.

II. INTERNET TECHNOLOGY

A. The Nature and Architecture of the Internet

The Internet is an international network of interconnected computers. These computers include host computers, which store and relay speech, and user computers, which upload, view, or download speech over the Internet. Three types of actors perform these Internet functions: (1) the sender or speaker; (2) the receiver or listener; and (3) the intermediary or service provider.[4] The relationship between the speaker and the intermediary allows the speaker to upload information to the host computer. The relationship between the listener and an intermediary allows the listener to view or download information posted by the speaker.

As a medium of communication, the Internet allows access to information that reflects the depth and breadth of human speech. Some Internet sites contain sexually explicit material, hate speech, libelous material, and material advocating illegal conduct. Other sites provide forums for political speech, allow global access to all types of information, and contain full-text versions of classic literature. And increasingly, the Internet is also a vehicle for commercial activity of many kinds.

B. Access to Information on the Internet

Individuals can access the Internet through a variety of sources including Internet Service Providers ("ISPs"), schools, employers, local libraries, and "cyber cafes." New methods of accessing the Internet are also likely to develop. For example, individuals can now access the Internet through cable lines and televisions or through wireless instruments such as cellular telephones and personal data assistants. Moreover, once users access the Internet, they can send and receive information in a variety of ways. For example, a user can transfer information through e-mail, list services, newsgroups, chat rooms, bulletin

4. *See id.* at 399.

boards, and the Web. As the Supreme Court noted in *Reno v. ACLU*, "these methods are constantly evolving and difficult to categorize precisely."[5]

Any of these transfer methods can accomplish mass distribution of information. Mail-exploders, list services, and newsgroups distribute information to a mass audience through e-mail.[6] These services place information into an individual's private e-mail account, usually without human intervention. The user simply enrolls in these services with an intermediary such as an ISP or a school, and the host computer automatically sends the information to the user without further human effort. Similarly, users of chat rooms and instant-messenger services voluntarily exchange typed messages in real time with others who visit the chat room or enroll in the messenger service.

A Bulletin Board Services ("BBS"), however, is slightly different. It operates on its own rather than through an intermediary, and a user must access the BBS independently of accessing any other information on the Internet. As a result, the BBS has a greater ability to dictate the terms of access to its system, and the user generally knows what information is being sought from the BBS.

Users can navigate the Web in one of three ways.[7] First, they can type the address of a particular site into a web browser. Second, they can run a search through one of the various search engines to obtain a list of sites containing the desired information. Third, they can connect through a web page that contains links to other web pages with similar information or to other sites of potential interest. Some websites place the information that they contain into the public domain without any charge to users. Other sites require users to obtain membership or to pay for the information.

Individuals and organizations, including the government and advocacy groups, can both publish and receive information on the Web. As the *Reno I* Court stated, the Web "constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers."[8] No single entity controls access to or membership on the Web, and there is no single point from which sites or services can be blocked.[9] An imprecise search for sites containing political speech, for example, could yield some sites containing sexually explicit material or hate speech. While this may be surprising for the searcher, most sites contain preliminary pages indicating

5. Reno v. ACLU, 521 U.S. 844, 851 (1997) ("*Reno I*").

6. *See id.*

7. *See id.*

8. *Id.* at 853.

9. *See id.*

the type of content on the site. Because of this feature, it is improbable that a user will accidentally access objectionable material.[10]

Finally, parents can control the types of sites their children access.[11] On the user end, for example, Microsoft's most recent Internet Explorer allows parents to limit children's access based on language, sex, nudity, and violence on various websites.[12] Moreover, users can purchase programs, such as Net Nanny, which allow them to prevent children from accessing certain sites based on content. On the sender's end, access to sites can be controlled through various age-verification programs that generally use credit card possession or digital certification services to ensure that the user has the requisite characteristics to enter the site. Vendors of programs that control access on the sender's end usually charge both senders and users for these services. Most casual Internet users are unwilling to pass through the barriers created by these vendors.[13]

C. Transfer of Information on the Internet

Users can transmit text, images, and sound over the Internet through the various methods of access described above. The user transmits code that represents the image or text. For example, once the receiver indicates a desire to download a picture, the computer storing the picture sends a copy of the binary code representing that picture to the receiver's computer. The receiver's computer then rebuilds the picture from the code.

There are two primary ways of receiving images and text on the Internet: downloading and viewing. If the user downloads the item, the computer saves a copy that the user can print, alter, or delete. If the user merely views the image, however, the computer will not save a copy unless the user takes affirmative steps to save it.

---

10. *See id.* at 854. Some unwanted exposure, however, is certainly possible. For example, a researcher trying to access information about the President could find it by typing in "www.whitehouse.gov." But only a small change — to "www.whitehouse.com" — would send the reader to a porn site, complete with pictures on the homepage.

11. *See id.*

12. This option is contained under "Content" in the "Internet Options" part of the Tools menu on Internet Explorer 6.0.

13. *See Reno I*, 521 U.S. at 857 n.23 (discussing the district court's findings to this effect).

Finally, the Internet has no geographical, land-based limitations. Thus, a receiver in Ashville, Tennessee can access an image stored on a computer in New York and controlled by a website operator in San Francisco. Moreover, with current technology, neither the host computer nor the website operator can determine the location of the receiver without requesting additional input from the receiver. Consequently, a website operator can post on the Internet an item that can be viewed throughout the world. But the website operator will not know who is accessing the material unless notified, sued, or charged with a crime. Thus, an operator could distribute speech to an illegal receiver without ever specifically intending to do so.

Future technological development will likely revolve around the ability of parties to identify users and block transmissions on the Internet. Technology currently exists allowing both senders and receivers to block some unwanted transmissions. Age verification and Net Nanny are examples of such technology. These technologies, however, are expensive, invasive, and less than perfect. The blocking tools available to senders are generally unavailable to all senders because of expense.[14] In addition, savvy children can avoid the blocking mechanisms available to receivers. Finally, the mechanisms available to the hosts are extraordinarily crude.[15]

More effective blocking would require greater information to be available to both senders and receivers of information. For effective blocking to take place from the sender's end, the sender needs to be able to identify certain characteristics about the receiver. One way to effect this change is through the development of a "passive identification code," which would allow the sender to identify salient characteristics about the receiver without requiring affirmative input. For effective blocking on the receiver's end, the receiver needs to have certain information about the content of the site. This would allow the receiver to seek out or avoid certain kinds of Internet content. But only a significant change in the technological architecture of the Internet can make this information available.[16]

14. *Id.* at 856-57.

15. *See* Lessig & Resnick, *supra* note 3, at 414 (explaining that these mechanisms generally allow an intermediary to block all website requests to a particular IP address, which is a series of numbers identifying a particular computer, or none of them).

16. *See id.* at 429-30.

III. REGULATION OF SPEECH ON THE INTERNET

People generally have two modes of engaging in mass communication: through in-person public speech and through the mass media. The Supreme Court's jurisprudence addresses both modes, providing different levels of constitutional protection to different locations and modes of communication. This section discusses the development of doctrines associated with the speech regulation and explains how these doctrines could apply to Internet speech. It argues that the Internet is entitled to full First Amendment protection.

A. Traditional Regulation of In-Person Speech

In *Perry Education Ass'n v. Perry Local Educators' Ass'n*, the Supreme Court established the basic framework for evaluating speech in a public forum.[17] The Court established a tripartite scheme in which the degree of First Amendment protection depends on where the speech takes place.

First, the Court considered traditional public forums such as streets and parks.[18] In these forums, any content-based restriction must satisfy strict scrutiny. The restriction must be necessary to serve a compelling state interest and must be narrowly tailored to achieve that end.[19] In addition, a state's content-based restrictions must also be the least restrictive means of accomplishing the government's interest.[20]

In contrast, any content-neutral restrictions — such as those regulating the time, place, or manner of communication — must satisfy intermediate scrutiny. Such a restriction must be "narrowly tailored to serve a significant government interest and must leave open ample alternative channels of communication."[21] *Perry's* second category applies when the government designates a nontraditional forum as "open."[22] In such a forum, restrictions on speech must satisfy the same tests that apply to traditional public forums.[23]

---

17. 460 U.S. 37 (1983).

18. *See id.* at 45.

19. *Id.* If the regulation takes into account the message that the regulated speech conveys, it is generally content based; otherwise the regulation is content neutral. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

20. *See Reno I*, 521 U.S. at 874.

21. *Perry*, 460 U.S. at 45.

22. *Id.*

23. *See id.* at 46.

Even in areas that are not public forum, by tradition or designation, the government may impose time, place, and manner restrictions as well as any other restrictions that "reserve the forum for its intended purposes, communicative or otherwise, as long as the regulation . . . is reasonable and not an effort to suppress speech simply because the government officials oppose the speakers' views."[24]

Through the years, the Court has taken these principles governing physical forums and applied them to various forms of mass media, from newspapers, to broadcast television and radio, to cable television. These media receive different degrees of protection, depending on their characteristics. The Court's next task will require applying these precedents to the evolving Internet medium.

B. Regulation of Mass Media

1. The Broadcast Medium

The government generally bears a lower burden in justifying speech restrictions on the broadcast medium than in justifying speech restrictions on other communications media.[25] In *Red Lion Broadcasting Co. v. FCC*, the Supreme Court addressed whether the FCC could impose on the broadcast medium "fairness doctrine" regulations, which force broadcasters to provide reply time to the subjects of personal attacks and political editorials.[26] The Court approved such regulations because the broadcast medium faces a scarcity problem.[27] Thus, "where there are substantially more individuals who want to broadcast than there are frequencies to allocate, it is idle to posit an unbridgeable First Amendment right to broadcast comparable to the right of every individual to speak, write, or publish."[28] Due to this problem, the government has a substantial interest in regulating access to the airwaves and in setting the rules for that access. Reviews of these regulations are not held to the traditional strict-and-intermediate scrutiny standards.

24. *Id.* at 45-46.

25. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 387 (1969).

26. *See id.* at 375.

27. *See id.* at 388.

28. *Id.*

The Supreme Court confronted a slightly different problem with respect for the broadcasters in *FCC v. Pacifica Foundation*.[29] In response to a complaint, the FCC determined that a radio broadcast of George Carlin's comedy routine entitled "Filthy Words" was indecent and prohibited by statute.[30] The Supreme Court upheld the FCC's action on the grounds that "the broadcast media have established a uniquely pervasive presence in the lives of all Americans."[31] The Court explained that indecent material broadcasted over the airwaves confronts citizens not only in public but also in their homes, where the right to be left alone outweighs the intruder's First Amendment rights.[32] Moreover, since listeners are constantly tuning in and out, prior warnings of upcoming content cannot completely protect them.[33]

The *Pacifica* Court also reasoned that broadcasting was "uniquely accessible" to children.[34] The Court noted that "other forms of offensive expression may be withheld from [children] without restricting the expression at its source. Bookstores and motion picture theaters, for example, may be prohibited from making indecent material accessible to children."[35] In summary, since the broadcast medium is "pervasive," content-based speech restrictions placed on the medium will be subjected to a lower standard of review. This rule has become known as the "pervasiveness doctrine."

2. The Print Medium

In contrast to the broadcast medium, the Supreme Court has given the print medium full First Amendment protection and has required any restrictions to be justified based on a higher standard.[36] In *Miami Herald Publishing Co. v. Tornillo*, for example, the Court struck down a right-of-reply statute similar to the one at issue in *Red Lion*.[37] In defense of the statute, access advocates argued that control of the print medium had become concentrated in a few national

29. 438 U.S. 726 (1978).

30. *See id.* at 732.

31. *Id.* at 748.

32. *See id.*

33. *See id.*

34. *Id.* at 749.

35. *See id.*

36. *See* Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 256-58, 260 (1974).

37. *Id.* at 247 (considering a statute that "provided a right of reply to press criticism of a candidate for nomination or election").

news organizations,[38] leaving the public without the "ability to respond or to contribute in a meaningful way to the debate on issues."[39] Furthermore, they argued that the number of competing newspapers had dwindled in many metropolitan areas.[40] The monopolization of the industry and the significant costs of startup created high barriers to entry — not just anyone could publish a newspaper.[41]

The Court rejected these arguments and held that government compulsion of a newspaper to publish "that which reason tells them should not be published is unconstitutional."[42] First, the Court noted that the right-of-reply statute exacted an improper content-based penalty against the paper.[43] Even though a newspaper is not constrained in terms of time, as is a broadcaster, it is constrained in terms of space.[44] Thus, the Court indicated that faced with the prospect of running afoul of the statute, a paper would forgo political coverage in favor of complying with the statute.[45] Second, the Court reasoned that even if the statute did not impose additional costs on the newspaper, the intrusion into the editor's function would still create First Amendment problems.[46] The Court held that the statute impermissibly regulated the editorial function of determining the size and the content of the publication.[47]

Thus, the *Tornillo* Court reaffirmed its rule that the print medium "is not a public utility subject to 'reasonable' governmental regulation in matters affecting the exercise of journalistic judgment."[48] Therefore, the lower standard of review for broadcast-medium regulations does not apply to the print medium — even though that medium is arguably more scarce than the broadcast medium. Nevertheless, the Court has allowed some regulation of the print

38. *See id.* at 249.

39. *Id.* at 250.

40. *Id.* at 249.

41. *Id.* at 251.

42. *Id.* at 256.

43. *See id.*

44. *See id.* at 256-57.

45. *See id.* at 257.

46. *See id.* at 258.

47. *See id.*

48. *Id.* at 259 (White, J., concurring).

medium by permitting the government to restrict minors' access to material deemed harmful to them.[49]

3. The Cable Medium

The Court has also refused to impose the lower standard enunciated in *Red Lion* to restrictions on the cable medium.[50] As the Court explained, "cable television does not suffer from the inherent limitations that characterize the broadcast medium," since "soon there may be no practical limitation on the number of speakers who may use the cable medium."[51] Regulation of cable broadcasts must therefore satisfy the requirements of strict scrutiny applied to traditional public forums and to print media.

In applying First Amendment tests to cable television, however, the Court is more likely to find a broader range of "substantial" or "compelling" state interests for regulating the cable industry than for regulating the print industry. For example, in *Turner Broadcasting System, Inc. v. FCC*, the Court considered whether the FCC can require cable operators to carry broadcast programming.[52] The Court held that the different physical characteristics of the cable medium should be taken into account when evaluating regulations of that medium.[53] This holding indicates that compelling state interests in regulation may differ for different communication media. As with the broadcast and print media, preventing minors' access to indecent speech is also a significant government interest in the cable medium.[54]

---

49. *See* Ginsberg v. New York, 390 U.S. 629, 641 (1968).

50. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 637 (1994). Content-neutral restrictions are subject to intermediate scrutiny, while content-based restrictions are subject to strict scrutiny. *Id.* at 642. There is no scarcity problem with the cable medium that would justify a lower standard for regulation. *Id.* at 639.

51. *Id.* at 638-39.

52. *Id.* at 637. "Must-carry" provisions require cable systems to set aside a portion of their channels for local broadcasters. *Id.* at 636.

53. *Id.* at 639.

54. *See* United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813-14 (2000).

C. The Internet as a Medium of Speech

Because the level of scrutiny for a particular type of speech varies based on the nature of the medium, characterizing the Internet medium will largely determine the validity of regulations imposed on Internet speech. This section compares the Internet with traditional media in an effort to assess the appropriate level of First Amendment protection.

1. Comparison of the Broadcast Medium to the Internet

While the Internet shares some characteristics with the broadcast medium, differences in the two media undercut the applicability of *Red Lion* and *Pacifica* to the Internet. As discussed above, the Court allows regulation of the broadcast medium on two primary grounds: scarcity of access for speakers and pervasiveness of broadcasts to the public. Scarcity does not affect the Internet in the way that airwave scarcity affects the broadcast medium. The *Red Lion* Court recognized that airwave scarcity required the government to limit the number of broadcast licenses; otherwise, competing speakers would drown each other out in an overcrowded field.[55] To ensure that broadcasters would not monopolize the content of the airwaves, the government could impose equal-access requirements to ensure that the "views and voices" of a community would be heard.[56] But because the Internet lacks a similar scarcity problem, the lower level of scrutiny applied to broadcast medium regulations should not apply to regulations of Internet speech.

The problem of pervasiveness of broadcast speech identified in *Pacifica* may also be an issue for the Internet. As with broadcast speech, unwanted material can invade the home when Internet users encounter such material online.[57] But in comparison to recipients of broadcast media, it is far less likely that Internet users will accidentally encounter objectionable material online.[58] To the contrary, an Internet user generally has to take affirmative steps to access such material, such as by running a search and selecting a site or a link.[59] Internet

55. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 388-89 (1969).

56. *Id.*

57. *See* FCC v. Pacifica Found., 438 U.S. 726, 748 (1978). An obvious example of this invasion is "spamming," whereby a receiver is inundated with unsolicited e-mails.

58. *See Reno I,* 521 U.S. at 854.

59. While accessing some websites causes unsolicited windows to open, it is highly unlikely that an Internet user who is visiting a nonobscene site would encounter an obscene pop-up window.

speech, therefore, is not pervasive in the same sense as broadcast speech. Instead, Internet speech invades less and warns more. As a result, the "pervasiveness doctrine" should not apply to the Internet.

2. Comparison of the Internet to the Public Forum, the Print Medium, and the Cable Medium

Essentially the same First Amendment analysis applies to speech restrictions on speech in public forums, in the print medium, and in the cable medium: Content-based regulations must meet the exacting requirements of the strict-scrutiny test, and content-neutral regulations must satisfy an intermediate level of scrutiny.[60] Yet the state's interest in regulating a particular type of speech varies by the nature of the forum. The state has a significant interest in maintaining public order when it regulates speech in public forums; thus, for example, it can impose time, place, and manner restrictions on a rock concert in a public forum.[61] In the cable medium, the state has a significant interest in maintaining the viability of the broadcast medium; thus, it can impose "must-carry" provisions requiring cable operators to carry certain programming.[62] Very few interests, however, are sufficiently compelling to allow the state to regulate the content of the print medium.[63]

The Internet shares certain characteristics of all three of these media types. Like a traditional public forum, it is generally accessible to the public. Like the cable medium, it can transmit sounds and moving images. Like the print medium, it can transmit text and images. But the Internet does not give rise to some of the problems of the public forum and the cable medium. For example, there is generally no need to maintain public order for a rock concert transmitted over the Internet. Furthermore, the Internet does not pose a significant threat to the viability of the broadcast medium. Therefore, the Internet currently most resembles the print medium for purposes of assessing significant government interests. As the Supreme Court recognized in *Reno I*, the Internet, unlike the broadcast medium, is entitled to full First Amendment protection.[64]

---

60. *See Turner*, 512 U.S. at 642.

61. *See Ward*, 491 U.S. at 792.

62. *See Turner*, 512 U.S. at 646-67.

63. *See Ginsberg*, 390 U.S. at 639-40. Of course, this latter interest is also applicable to the cable and broadcast media.

64. *Reno I*, 521 U.S. at 870.

The nature of the Internet as a medium, however, is still evolving. Technological advances may change the way that the Court views the Internet as a medium of speech. As technology evolves, so do the issues that could potentially warrant greater government regulation. Thus, even though the Internet now resembles the print medium, this similarity could change. If, for example, technological advances caused the Internet to threaten the continued existence of traditional broadcast media, then the Internet might more closely resemble the cable medium. Indeed, there is evidence of such a trend — Internet access has been offered by cable providers through cable lines. Changes in the technology or social context of Internet usage could change the interests that the Court deems compelling or substantial under its varying scrutiny standards. Currently, however, the Court has not found any such interests beyond that of helping parents regulate their children's access to indecent content.[65]

Assuming that the Internet is entitled to the full First Amendment protection as a public forum and that few interests in regulating it will be considered compelling, this article will next examine the problems inherent in applying traditional free-speech analysis to Internet communication.

IV. CONTENT-BASED RESTRICTIONS ON INTERNET SPEECH

A. The Obscenity Doctrine

1. Traditional Obscenity Law

Despite the fact that obscene speech is nevertheless speech, the Court has allowed governments to prohibit obscenity without running afoul of the First Amendment. But such prohibitions are allowed only if "obscenity" is clearly defined. In *Miller v. California*, the Supreme Court addressed the definition of obscene speech.[66] There, the Court held that state regulations of speech deemed obscene may be applied only to those depictions or descriptions of sexual conduct that are specifically defined by the statute.[67] In addition, the state must limit its proscription to works that depict or describe sexual conduct in a patently offensive way and that, taken as a whole, lack "serious literary, artistic, political or scientific value."[68]

65. *See id.* at 869-70.

66. 413 U.S. 15, 24 (1973).

67. *See id.*

68. *Id.*

The *Miller* Court established this three-part test for the trier of fact:

> (a) whether the average person applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interests . . . (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[69]

In *Miller*, the Court refused to articulate a national obscenity standard; instead, the Court incorporated local community standards in evaluating speech.[70] As the Court explained, "it is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City."[71] Thus, under the *Miller* test, commercial Internet distributors are subject to state law and to local community standards in the places where they distribute their speech.[72] Identical speech may therefore be protected in some communities because it is not obscene under local standards, but prohibited in others where, under local standards, it is considered obscene.

The Supreme Court has applied this reasoning to media services that are made available nationwide. In *Sable Communications of California v. FCC*, the Court affirmed the obscenity-based prosecution of a dial-a-porn company named Sable, holding that the Federal Communications Act of 1934 incorporated local obscenity standards.[73] The Court also noted that federal statutes are not rendered unconstitutional because distributors face varying standards in the jurisdictions into which they transmit their material.[74] The Court rejected Sable's argument that the Act placed distributors in the "double bind" of having to "tailor . . . their messages to the least tolerant community."[75] According to the Court, Sable

---

69. *Id.*

70. *See id.* at 30-32.

71. *Id.* at 32. A more interesting issue in the Internet context is whether the people of Las Vegas or New York City may be effectively denied access to all materials other than those found tolerable in Maine and Mississippi.

72. *See id.* at 27.

73. 492 U.S. 115, 124-25 (1992).

74. *See id.* at 125.

75. *Id.* at 124.

could instead comply with the Act by selectively tailoring its messages to individual communities. In addition, it could either devise a way to determine the source of incoming calls or block all out-of-area calls. The Court did not find it significant that Sable would be required to incur additional costs in implementing such a system.[76] Thus, as a rule, the distributor of the material bears the burden of complying with applicable community standards.[77]

In summary, the definition of "obscenity" under *Miller* is determined on a community-by-community basis. Furthermore, a distributor may be held liable under the varying standards of the states into which the material is transmitted.[78]

2. Obscenity Law on the Internet

As discussed above, the Internet knows no geographical boundaries, and website operators generally do not know the identity, age, or location of those who access their sites. This same problem characterizes e-mail systems, list services, and newsgroups. The Supreme Court in *Miller*, however, established a test for obscenity that centered on community standards in the jurisdiction of destination.[79] Furthermore, the *Sable* Court held that the speech distributor had the burden of ensuring compliance with the various standards in the receiving communities.[80]

Applying the *Miller/Sable* test for obscenity to Internet speech raises significant concerns for Internet speakers. Although recipients are inherently unidentifiable, application of the existing media standards would place responsibility on distributors of Internet speech to ensure that their speech met all community standards of all the potential recipients. Thus, under existing law, Internet speakers would be required to tailor their speech to the most restrictive community standard to ensure compliance with all state obscenity laws. Unless a website owner has the technology to target specific content to specific Internet users, it will be forced to limit its speech to whatever is nonobscene everywhere. In other words, the location with the most expansive definition of obscenity will provide a national standard for obscene speech. And receivers elsewhere will be deprived of speech that would otherwise be legal in their communities.

---

76. *See id.*

77. *See id.* at 126.

78. *See id.*

79. *See* Miller v. California, 413 U.S. 15, 24 (1973).

80. *See Sable*, 492 U.S. at 125-26.

From the standpoint of federal enforcement, two primary statutes prohibit the transportation of obscene material across state lines. Section 2252(a) of Title 18 prohibits the interstate transportation of child pornography,[81] and section 1465 prohibits the knowing or intended interstate transportation of materials such as an "obscene book, pamphlet, picture, film, paper, letter, writing, print, silhouette, drawing, figure, image, cast, phonograph recording, electrical transcription, or any other article capable of producing sound, or any other matter of indecent or immoral character."[82]

At least two courts have addressed the prima facie issue of whether the actual or intended transfer of computer files across state lines constitutes transportation.[83] In *United States v. Thomas*, a California BBS operator and his wife posted graphical image file ("GIF") pictures of arguably obscene sexual images.[84] An investigating postal inspector accessed the pictures in Tennessee. In a Tennessee federal district court, the defendants were convicted of interstate transportation of obscene material.[85]

On appeal, the defendants argued that transferring GIF images did not constitute transferring obscene material within the meaning of section 1465.[86] The Sixth Circuit, however, disagreed.[87] Even though the material was only binary code during the actual transfer, the court held that the transfer violated the statute because the content began as an obscene picture in California and ended as an obscene picture in Tennessee.[88] Based on the plain language of the statute, which used the words "distribution," "picture," "image," and "electrical transcription," the court concluded that the statute's scope included the transfer of Internet material over telephone lines.[89] Thus, under *Thomas*, the transfer of

81. *See* 18 U.S.C. § 2252A.

82. *See* 18 U.S.C. § 1465.

83. *See* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996) (addressing 18 U.S.C. § 1465); *cf.* United States v. Carroll, 105 F.3d 740 (1st Cir. 1997) (holding that the posting of child pornography on the Internet constituted evidence of intent to transport pictures in interstate commerce).

84. *See Thomas*, 74 F.3d at 705.

85. *See id.*

86. *See id.* at 706.

87. *See id.* at 707.

88. *See id.*

89. *See id.* at 709 (quoting United States v. Maxwell, 42 M.J. 568, 580 (A.F. Ct. Crim. App. 1995)).

files from a California BBS into Tennessee over telephone lines fell within the intent of Congress "to legislate comprehensively the interstate distribution of obscene materials."[90]

In *United States v. Carroll*, in arguing that the defendant had intended to engage in interstate commerce under 18 U.S.C. § 2252(a), the government relied partly on evidence that he had intended to post sexually graphic images of his 13-year-old niece on the Internet.[91] The evidence consisted of the niece's testimony that her uncle had told her about his plans to distribute the photographs on the Internet. The First Circuit held that evidence of such a plan, along with an inference that the pictures were taken across state lines to be developed, would have allowed a jury to reasonably infer that Carroll had intended to distribute child pornography in interstate commerce.[92]

A related issue is whether the receiver of child pornography can also be held responsible for transporting child pornography in interstate commerce.[93] In *United States v. Mohrbacher*, the government prosecuted a California resident who had downloaded child pornography from a BBS in Denmark.[94] The federal district court convicted Mohrbacher of one count of transporting visual depictions of minors engaging in sexually explicit conduct in violation of section 2252(a)(1).[95] The trial court reasoned that Mohrbacher had transported the materials because he had initiated the download from the BBS rather than passively receiving the pictures.[96]

The Ninth Circuit disagreed and held that a person who downloads an image from a BBS takes action that is more analogous to receiving material ordered by telephone than to shipping the materials.[97] To hold otherwise, the court explained, would "eliminate the distinction" between sellers/senders and buyers/receivers.[98] The Ninth Circuit rejected the government's reliance on

90. *See id.*

91. *See Carroll*, 105 F.3d at 742.

92. *See id.* at 742-43.

93. *See* United States v. Mohrbacher, 182 F.3d 1041, 1044 (9th Cir. 1999).

94. *See id.*

95. *See id.* at 1044, 1046.

96. *See id.* at 1046.

97. *See id.* at 1050.

98. *See id.*.

18 U.S.C. § 2(b), which allows "offenders who use innocent agents to perform illegal acts to be punished as principals."[99]

In *Mohrbacher*, the government's theory was that a customer who orders illegal materials from a supplier actually *causes* the supplier's illegal act of filling the order — in the same way that offenders "induce innocent parties to mail contraband on their behalf."[100] But the Ninth Circuit concluded that the government's interpretation of the statute would "vest unconstrained discretion in prosecutors . . . and might unwittingly render many provisions of criminal statutes superfluous or duplicative."[101] Finally, the court indicated that other jurisdictions have likewise limited section 2252(a)(1) prosecutions for the offense of shipping or transporting child pornography over the Internet to those who have either sent the material electronically to another computer or made the material available through a BBS or newsgroup.[102]

The laws prohibiting transportation of child pornography and obscene materials also require a *mens rea* of intentional or knowing interstate transportation.[103] It remains to be seen, however, whether a California website operator knowingly distributes obscene material in Tennessee when he or she has no knowledge that people in Tennessee have accessed or will access the website. The California website operator takes no action specifically aimed at Tennessee, and current Internet technology does not allow passive identification of the recipients. In fact, the website operator may even place disclaimers on the site to deter access in Tennessee. If Tennessee residents nevertheless access the materials, then the question arises whether the California website operator has knowingly transported obscene materials.

In some situations, Internet sites require registration or membership, giving their operators specific information about their subscribers and enabling the government to more easily show intent to transport the material across state lines. In *Thomas*, a Tennessee federal district court convicted a California

99. *Id.* (citing and paraphrasing the holding of United States v. Causey, 835 F.2d 1289, 1292 (9th Cir. 1987)).

100. *See id.* at 1050-51 (noting the government's reliance on United States v. Thomas, 893 F.2d 1066 (9th Cir. 1990)).

101. *Id.* at 1051.

102. *See id.* (citing cases from the First, Second, Fifth, Sixth, and Eleventh Circuits for this proposition, and citing cases from the Fifth, Seventh, and Tenth Circuits for the proposition that prosecution for downloading child pornography is properly brought under § 2252(a)(2) and/or 2252(a)(4), which prohibit *possession* of the materials).

103. *See* 18 U.S.C. §§ 1465, 2252(a).

resident for allowing his BBS to send obscene images into Tennessee.[104] The Sixth Circuit held that prosecution in Tennessee, applying Tennessee's local community standards of obscenity, was proper because Thomas could have prevented access by Tennessee residents.[105]

Thomas had required users of his BBS to provide information, including their addresses, before receiving a password that would provide access to the material at issue. The court reasoned that Thomas could have simply denied passwords to people in jurisdictions where his material was illegal.[106] This reasoning, the court noted, comports with *Sable*.[107] Since Thomas was a commercial distributor of material, he had the ability to screen where he sent the material. He therefore had the responsibility to determine where his material was illegal and the responsibility to block transmissions to those jurisdictions.[108]

Thomas was a simple case. Any individual who has an Internet communications device that requires receivers to provide their location can be charged in a receiver's state for violations of obscenity laws. Furthermore, since BBS systems are remote dial-in facilities — that is, receivers have to call them separately — incoming calls can possibly be screened based on area codes.[109]

Unlike BBSs, however, websites are not remote dial-in facilities. Receivers of information on the Internet dial into a host computer and then have the ability to go anywhere anonymously. Website operators who do not require the affirmative input of information do not know the jurisdiction of those who access their material.[110] Thus, to avoid criminal liability in a jurisdiction that

104. *See* United States v. Thomas, 74 F.3d 701, 705-06 (6th Cir. 1996).

105. *See id.* at 710-11.

106. *See id.*

107. *See id.* at 711-12; *see also* Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 125-26 (1989).

108. *See Thomas*, 74 F.3d at 711.

109. *Cf. id.* at 711 (noting that address and telephone number were provided on the application form).

110. The technology to provide website operators with geographic information about those who visit the site is evolving, but it is still in early stages of development. *See generally* Matt Richtel, *High Stakes in the Race to Invent a Better-Blocker*, N.Y. TIMES, June 28, 2001, *available at* http://www.nytimes.com/2001/06/28/technology/28GAMB.html; Stefanie Olsen, *Yahoo Ads Close in on Visitors' Locale*, June 27, 2001, CNETNEWS.COM, *at* http://news.cnet.com/news/0-1005-200-6397360.html (Yahoo signed deal to send consumers specific online ads based on where they live or work); Michael Geist, *E-borders Loom, for Better or Worse*, THE GLOBE & MAIL, June 28, 2001, *available at* http://newes.globetechnology.com/servlet/GAMAArticleHTML.

they did not know they were reaching, these operators have three options: (1) require the affirmative input of information, (2) tailor their content to the most restrictive jurisdiction, or (3) choose not to speak.[111]

Most websites cannot afford to obtain affirmative input from users and to screen users by location.[112] Even if website operators could afford to implement such procedures, any law requiring such procedures would have a chilling effect on speech since some users, based on privacy concerns, would refuse to access the sites. The second option, tailoring content to the most restrictive jurisdiction, is possible. But requiring a website to do so may violate the First Amendment by restricting speech that is legal in some jurisdictions.

Furthermore, posting warnings and disclaimers on the website may well be ineffective.[113] *Thomas* does not bode well for website operators with such disclaimers. Indeed, *Thomas* teaches that operators with the capacity to identify a receiver's home state may be prosecuted for the website's content in the receiver's jurisdiction.[114]

B. The Indecency Doctrine

Like the obscenity doctrine, the indecency doctrine is difficult to apply to Internet speech because distributors have limited ability to identify the recipients of their speech. Under the obscenity doctrine, the key characteristic to identify is the recipient's location; under the indecency doctrine, the key characteristic to identify is the recipient's age. The development of a passive-identification technology might remedy this problem. This section discusses the development of traditional indecency principles, governmental attempts to regulate indecency on the Internet, and a proposed solution to indecency on the Internet.

111. *See Thomas*, 74 F.3d at 711-12.

112. *But cf. Sable*, 492 U.S. at 125-26 (holding that there is no constitutional impediment to forcing Sable to incur some costs).

113. As a practical matter, most sexually oriented websites post disclaimers indicating the content of the site and commanding that people residing in jurisdictions where that content is illegal not enter the site.

114. *See Thomas*, 74 F.3d at 710-11. To be constitutitonal, the applicable obscenity law would, of course, have to comport with the *Miller* test.

1. Traditional Indecency Law

The First Amendment protects sexual expression that is indecent but not obscene.[115] Even so, a state may regulate indecent speech if the regulation promotes a compelling state interest and is the least restrictive means of furthering that interest.[116] States have been held to have a compelling interest in shielding minors from indecent speech,[117] and many of the Supreme Court's indecency cases involve legislation that restricts "indecent" speech in an effort to protect children. In *Ginsberg*, the Court upheld the following definition of "harmful to minors:"

> "Harmful to minors" means that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:
>
> (i) predominantly appeals to the prurient, shameful or morbid interest of minors, and
>
> (ii) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors, and
>
> (iii) is utterly without redeeming social importance for minors.[118]

Despite the state's authority to regulate indecent speech, the *Ginsberg* Court emphasized that the primary responsibility for the custody, care, and nurture of children rests with their parents.[119] Thus, government regulation should attempt only to assist parents in this responsibility, not to prohibit the communication entirely.[120] The central conflict in the indecency cases is the law's ability to protect children without unduly restricting adult access to the materials.

---

115. *See Sable*, 492 U.S. at 126.

116. *See id.* Regulations of indecent speech are subject to strict scrutiny because they regulate the content of speech.

117. *Id.* (citing *Ginsberg* 390 U.S. at 639-40).

118. *Ginsberg*, 390 U.S. at 643, 646.

119. *Id.* at 639 (quoting Prince v. Massachusetts, 321 U.S. 158, 166 (1944)).

120. *See id.* at 640.

In trying to shield children from indecent speech, Congress has a habit of "burn[ing] the house to roast the pig,"[121] and the Supreme Court has often found such regulatory efforts unconstitutionally overbroad. In *Sable*, for example, the Court invalidated section 233(b) of the Communications Act of 1934 because the Act prohibited the interstate transmission of indecent as well as obscene speech.[122] Since the provision established a total ban on indecent telephone messages — speech that adults have a right to receive — the regulation was not the least restrictive means of limiting children's access to indecent speech.[123]

Similarly, in *United States v. Playboy Entertainment Group, Inc.*,[124] the Court struck down section 505 of the Telecommunications Act of 1996, which required cable operators that provide indecent material either to "scramble" or fully "block" those channels or to limit transmission to times when children are probably not viewing.[125] In an effort to comply with these requirements, cable operators fully blocked the transmission of sexually explicit channels for two-thirds of the day. This practice resulted in blocking regardless of whether children were present or likely present and regardless of the wishes of adult viewers.[126]

Cable channels that provide sexually explicit programming challenged these regulations. The Supreme Court, quoting its 1971 opinion in *Cohen v. California*, explained: "Where the designed benefit of a content-based speech restriction is to shield the sensibilities of listeners, the general rule is that the right of expression prevails, even where no less restrictive alternative exists. We are expected to protect our own sensibilities 'simply by averting [our] eyes.'"[127] While the Court found a compelling governmental interest in protecting children from the broadcasts, the Court rejected the requirement that channels be blocked completely at certain hours, concluding that less restrictive alternatives were available.[128]

---

121. Butler v. Michigan, 352 U.S. 380, 383 (1957), *quoted in Sable*, 492 U.S. at 131.

122. *See Sable*, 492 U.S. at 131.

123. *See id.* at 128-29, 131.

124. 529 U.S. 803, 813-14 (2000).

125. *Id.* at 812-27.

126. *See id.* at 812.

127. *Id.* (bracket in original) (quoting Cohen v. California, 403 U.S. 15, 21 (1971)).

128. *See id.* at 811.

As the Court explained, cable operators have the ability to "block unwanted channels on a household-by-household basis."[129] The Court found that the government had not proved that the household-by-household blocking option was ineffective in achieving the government's goal of supporting parents who wanted the channels blocked.[130]

2. Indecency Law on the Internet

Indecency online bothers Congress. In its zeal to help parents shield children from online indecency, Congress enacted questionable legislation — provisions of the Communications Decency Act ("CDA")[131] — which the Supreme Court promptly struck down.[132] Congress's most recent effort in this arena is the Child Online Protection Act ("COPA"),[133] as discussed below.

a. The Communications Decency Act

Two provisions of the CDA were challenged soon after the President signed them. The first, 47 U.S.C. § 223(a), prohibited the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provided for a fine under Title 18, or imprisonment for not more than two years, or both, against any person who:

> (1) in interstate or foreign communications —
>
> . . . .
>
> (B) by means of a telecommunications device knowingly —
>
> (i) makes, creates, or solicits, and
>
> (ii) initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age,

129. *Id.* at 815 (distinguishing FCC v. Pacifica Found., 438 U.S. 726, 744 (1978), on the basis that broadcast did not have a similar blocking mechanism).

130. *See id.* at 816-27.

131. 47 U.S.C. § 223 (a), (d); *see also* S. REP. 104-358 (1996).

132. *See Reno I,* 521 U.S. at 885.

133. Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified at 47 U.S.C. § 231).

> regardless of whether the maker of such communication placed the call or initiated the communication [or]
>
> (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity . . . .[134]

The second provision, 47 U.S.C. § 223(d), prohibited the knowing sending or displaying of patently offensive messages in a way that made it available to a person under 18 years of age. Again, it provided for a fine under Title 18, or imprisonment for not more than two years, or both, against any person who:

> (1) in interstate or foreign communications knowingly —
>
> (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
>
> (B) 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; or
>
> (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity.[135]

The statute also provided two affirmative defenses. The first defense applied to those who take "good faith, reasonable, effective, and appropriate actions" to restrict minors from accessing the prohibited communications. The other applied to those who restrict access to prohibited material through various forms of age proof, such as a verified credit card or an adult identification number or code.[136]

---

134. 47 U.S.C. § 223(a).

135. 47 U.S.C. § 223(d).

136. 47 U.S.C. § 223(e)(5)(A), (B); *see also Reno I*, 521 U.S. at 881.

b. Reno v. ACLU (Reno I)

The American Civil Liberties Union ("ACLU") immediately challenged the constitutionality of the CDA, and a three-judge panel of the United States District Court for the Eastern District of Pennsylvania enjoined the enforcement of section 223(a)(1)(B) insofar as it applied to "indecent speech" and enjoined the enforcement of sections 223(d)(1)-(2) completely.[137] On direct appeal, the Supreme Court affirmed the trial court's judgment.[138]

The government cited three of the Supreme Court's precedents in arguing that the CDA was constitutional, but the Court distinguished all of them.[139] First, the Court reasoned that the statute upheld in *Ginsberg v. New York* was much narrower than the CDA.[140] Second, the Court distinguished *FCC v. Pacifica Foundation* because: (1) the order in *Pacifica* targeted a particular broadcast rather than a broad range of speech; (2) a federal agency familiar with the broadcast industry issued the order in *Pacifica*; and (3) the broadcast medium had a history of regulation.[141] Finally, the Court distinguished *Renton v. Playtime Theatres, Inc.* by rejecting the government's argument that the CDA was "cyberzoning."[142] Unlike the content-neutral restriction that was aimed at "secondary effects" in *Renton*, the CDA was a content-based restriction aimed at regulating the primary effects of speech; therefore, the CDA should not be analyzed as a mere time, place, or manner restriction.[143]

---

137. ACLU v. Reno, 929 F. Supp. 824, 883 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

138. *Reno I*, 521 U.S. at 849.

139. *Id.* at 864 (distinguishing Ginsberg v. New York, 390 U.S. 629 (1968), FCC v. Pacifica Found, 438 U.S. 726 (1978), and Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986)).

140. *Id.* at 865 (explaining that the statute in *Ginsberg* was narrower in four ways: (1) it allowed parents to purchase the regulated material for their children while the CDA did not; (2) it applied only to commercial transactions while the CDA contained no such limitation; (3) it defined "indecent" or "patently offensive" as being without serious literary, artistic, political, or scientific value while the CDA did not; and (4) it applied only to children under 17, while the CDA applied to those under 18.

141. *Id.* at 867.

142. *Id.* at 868.

143. *Id.*

The Court then drew a sharp distinction between the broadcast medium and the Internet. It noted that the Internet is not as "invasive" as radio or television since images do not appear on the computer screen unrequested and since users seldom encounter content by accident.[144] The Court also noted that the Internet is not a scarce commodity because it provides a relatively unlimited capacity and a low-cost method for communication.[145] Thus, the Court concluded that "the content of the Internet is as diverse as human thought" and that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[146]

Having identified the appropriate constitutional test, the Court applied it and held that the CDA was unconstitutionally vague.[147] The Court reached this conclusion in part because the statute did not define the words "indecent" or "patently offensive."[148] The absence of such definitions would inevitably lead to "uncertainty among speakers" about the two provisions' relationship and meaning.[149] The Court stated that the CDA's vagueness was of special concern for two reasons: (1) it was a content-based restriction on speech; and (2) it was a criminal statute.[150] For these reasons, the Court believed that the statute would have a significant chilling effect since it presented a threat of censoring speech that would fall outside the statute's scope.[151]

The Court also held that the statute was facially overbroad, penalizing speech that should have been protected. In its attempt to deny minors access to

144. *Id.* at 869.

145. *Id.* at 870.

146. *Id.*

147. *Id.* at 874.

148. *Id.* at 871.

149. *Id.*

150. *Id.* at 871-72.

151. *Id.* at 874. In trying to save the statute, the government argued that the statute was no more vague than *Miller*'s obscenity standard because the "patently offensive" definition contained in the statute was part of Miller's obscenity definition. *Id.* at 872-73. The Court rejected this argument because the statute did not contain the limitations placed on the definition by the second and third prongs of the *Miller* definition. *Id.* at 873. Moreover, the Court noted that the definition in *Miller* was limited to depictions of sexual conduct, but no similar limitation was contained in the CDA. *Id.*

potentially harmful speech, the statute suppressed a large amount of speech that adults were constitutionally entitled to receive.[152] The Court reiterated that regardless of the strength of the government's interest in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox."[153] Moreover, just because some members of the population find the speech offensive is not a sufficient reason to suppress it.[154] The Court agreed with the district court that the CDA resembled the ban struck down in *Sable*.[155]

In holding that the CDA was overbroad, the Court rejected the government's argument that prohibiting transmission whenever one party is known to be a minor would not interfere with adult-to-adult communication.[156] The Court saw the problem as twofold. First, there was no way for websites to prohibit minors from accessing indecent material without also preventing access by adults.[157] Second, there was no way for speakers to determine the age of people accessing material through chat rooms, mail exploders, e-mail, or newsgroups.[158] Thus, the Court tied its decision to the technology existing in 1997. By implication, if it becomes feasible for website operators to identify recipients, a child-targeted indecency regulation could be upheld.[159]

Finally, the Court emphasized the "unprecedented" breadth of the CDA.[160] It noted that the CDA applied to all individuals, nonprofit entities, and commercial entities.[161] The undefined terms "indecent" and "patently offensive" could cover large amounts of educational or socially valuable material.[162] As the Court observed, the statute could even cover the card catalogue of the Carnegie

152. *Id.* at 874.

153. Bolger v. Young's Drug Prods. Corp., 463 U.S. 60, 74 (1983), *quoted in Reno I*, 521 U.S. at 875.

154. *Reno I*, 521 U.S. at 875.

155. *Id.*

156. *Id.* at 876.

157. *Id.* at 876-77 (stating that it would be prohibitively expensive for noncommercial and some commercial speakers to verify that website users are adults).

158. *Id.* at 876.

159. *See id.* at 875-77.

160. *Id.* at 877.

161. *Id.* The prohibitions at issue in *Ginsberg* and *Pacifica* covered only commercial speech and commercial entities.

162. *Id.*

Library.[163] Given the broad, content-based coverage of the CDA, the government carried a heavy burden to explain why a less restrictive provision would not be as effective as the CDA; the government failed to meet this burden.[164]

In summary, the Court imported into the Internet context most of its jurisprudence concerning the overbreadth and vagueness doctrines, as well as its jurisprudence regarding indecency in the cable and print media. Justice O'Connor, concurring in part and dissenting in part, was more reticent about distinguishing the Court's zoning cases.[165] She noted that although not feasible at the time, "it is possible to construct barriers in cyberspace and use them to screen for identity" and that this transformation was under way.[166] Thus, she suggested that the Court should move carefully and should wait for the technology to develop before making any large pronouncements.

c. The Child Online Protection Act

After the Court struck down the CDA, Congress enacted COPA, which was much more narrowly drawn than the CDA. For example, 47 U.S.C. § 231(a)(1) states:

> 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.[167]

The statute excludes from coverage telecommunications carriers engaged in the provision of telecommunications services, persons providing Internet access services, and persons providing Internet search services.[168] The statute

163. *Id.*

164. *Id.* at 879. For example, the government failed to explain how the "tagging" of material so that parents could control the content of material coming into their homes would be less effective. *Id.* In addition, the Court held that the statute could not be severed to correct its facial overbreadth. *See id.* at 882-85.

165. *See id.* at 886-87.

166. *Id.* at 890-91 (explaining that speakers could eventually use these barriers to identify the age of receivers, and receivers could also limit the information they receive by using various programs or a browser's screening ability).

167. 47 U.S.C. § 231(a)(1).

168. 47 U.S.C. § § 231(b)(1)-(3).

also excludes from coverage any person engaged in the transmission, storage, retrieval, formatting, or translation of a communication made by another person, without selection or alteration of that communication's content.[169] Further, the statute provides for an affirmative defense if the defendant:

> in good faith, has restricted access by minors to material that is harmful to minors —
>
> (A) by requiring the use of a credit card, debit account, adult access code, or adult personal identification number;
>
> (B) by accepting a digital certificate that verifies age; or
>
> (C) by any other reasonable measures that are feasible under available technology.[170]

Finally, the statute contains a list of limiting definitions. For example, it defines "commercial purposes" as engaging in the business of making communications over the Internet.[171] It also defines "engaged in business" as having the objective of earning a profit.[172] Moreover, a person is "engaged in business" under the statute only if he or she either knowingly causes or knowingly solicits material that is harmful to minors for posting on the Web.[173] Finally, COPA defines "material that is harmful to minors" as:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter . . . that is obscene or that —
>
> (A) the average person, applying community standards, would find, taking the material as a while and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> (B) 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

169. 47 U.S.C. § 231(b)(4).

170. 47 U.S.C. § 231(c)(1).

171. 47 U.S.C. § 231(e)(2)(A).

172. 47 U.S.C. § 231(e)(2)(B).

173. *Id.*

sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.[174]

Being clearly narrower than the CDA, COPA limits itself to commercial website operators and contains a much more precise definition of "indecent" material. Nonetheless, it does not address the often emphasized limitation on the ability of distributors to identify the recipients of their speech.

d. ACLU v. Reno (Reno II)

Although Congress took the Court's advice and drafted a much narrower statute, a Pennsylvania federal district court entered a preliminary injunction against the statute,[175] and the Third Circuit upheld this decision.[176] The Third Circuit concluded that COPA is a content-based restriction and is therefore presumptively invalid and subject to strict scrutiny.[177] The court found that the government has a compelling state interest in protecting children from harmful material, even if that material is not obscene.[178] Thus, the issue was whether the statute satisfies the other requirements of strict scrutiny.[179]

The court held that COPA does not satisfy strict scrutiny because its reliance on the "community standards" language in *Miller* made the statute over-broad when applied to the Internet.[180] The court based its decision on the "crucial differences between a 'brick and mortar outlet' and the online Web that dramatically affect a First Amendment analysis."[181] First, the Web is not geographically contained.[182] Thus, Web publishers are without means to limit

174. 47 U.S.C. §§ 231(e)(6)(A)-(C).

175. ACLU v. Reno, 31 F. Supp. 2d 473, 498-99 (E.D. Pa. 1999).

176. ACLU v. Reno, 217 F.3d 162, 174-75 (3d. Cir. 2000) (*"Reno II"*), *vacated and remanded sub nom.* Ashcroft v. ACLU, 122 S. Ct. 1700 (2002).

177. *Id.* at 167.

178. *Id.* at 166.

179. *Id.*

180. *Id.* at 173-74 (noting that the parties did not raise this argument in the district court or in their briefs).

181. *Id.* at 175.

182. *Id.*

access to their sites based on the geographic locale of Internet receivers.[183] Second, due to the nongeographic nature of the Web, every Web publisher would have to censor its publication severely or place its publication behind an age or credit-card verification shield in order to avoid violating COPA.[184] Such shielding would place a burden on adults receiving speech to which they are entitled. It would also prevent minors (those under age 17) from accessing material that is legal in their community simply because such material is illegal in other communities.[185] The Third Circuit recognized these technological burdens and held that neither a community-standards test nor an affirmative age-verification requirement could withstand strict scrutiny.

The Supreme Court recently reversed the Third Circuit's judgment in *Reno II*, holding that COPA's reliance on "community standards" to identify material that is harmful to minors does not, in itself, render the statute substantially overbroad.[186] The Court, however, expressed no view about other issues raised in the Third Circuit, including: (1) whether COPA suffers from substantial overbreadth for reasons other than its use of community standards; (2) whether COPA is unconstitutionally vague; or (3) whether COPA survives strict scrutiny.[187] Leaving the preliminary injunction undisturbed, the Court remanded the case to the Third Circuit to "examine these difficult issues."[188]

V. A PROPOSED GENERAL APPROACH TO SPEECH ISSUES ON THE INTERNET

In the regulation of Internet speech, the question is often the same: Was the website operator able to identify the location or age of the recipient of the speech? If so, the operator can be more easily be held liable for violations of either community standards or age-based obscenity and indecency laws. If not, the operator may be allowed to argue that limits on speech are overbroad because they prohibit communications that are protected by the First Amendment.

183. *Id.*

184. *Id.*

185. *Id.*

186. Ashcroft v. ACLU, 122 S. Ct. 1700, 1713 (2002).

187. *Id.*

188. *Id.* at 1713-14.

One architectural limitation of the Internet presents an obstacle to importing traditional free-speech doctrines: the inability of Internet speakers to passively identify the recipients of their speech. To the contrary, they must request affirmative input from recipients to ascertain this information. While such input allows greater control over recipients, it also chills speech.

Two possible technological developments could allow a better tie between Internet speakers and audiences. One is the development of a passive-identification code that provides websites with automatic information about visitors — such as age and geographic origin. The second is the designation of the Internet as a "free speech zone" in which speakers would "tag" potentially objectionable content and recipients would be responsible for avoiding unwanted communications. Because the creation of a passive-identification code would dissuade Internet speech by creating burdens for both speakers and receivers, the development of "tagging" technology provides a better solution.

A. Regulators of Speech and Passive-Identification Code

There are four regulators of speech: social norms, the market, the architecture of forum, and the law.[189] All are present in the Internet context and can either complement or oppose one another. Further complicating matters is the fact that only computer code *directly* regulates the Internet. And private entities, which generally need incentives to act, control the development of computer code. Consequently, while the government can try to force these private entities to enact regulating code, enforcing such regulations would be difficult. Given the speed of technological change and the difficulties of policing the Internet, the government can often be most effective by creating incentives for technology to develop in a particular way.

Code that allows Internet speakers to identify certain characteristics about the receivers would effectively enable regulation on the Internet. Under the traditional First Amendment framework for obscenity and indecency, the characteristics that must be identified are age and location. Speakers need this information to conform their speech to the law.

The four modalities of regulation must respond to this need. The market pushes in favor of such code. The ability to identify the age and location of recipients would be a powerful tool for an online marketer. If the marketer could make these identifications, it could tailor its site to each user. For example, if a six-year old girl logs onto the site, the marketer could advertise dolls on the first page. A website visitor who has booked a ski trip on one site might be offered ski boots on another. Online marketers have already begun collecting and selling information about the browsing and buying habits of website visitors.

---

189. *See* LESSIG, *supra* note 3. For a discussion of these regulators and how they generally relate to cyberspace, see *id.*, Chapter 5.

Current American social norms about anonymity on the Web are more ambivalent. These norms allow the complete proscription of obscene speech and the regulation of indecent speech. Furthermore, these norms seem to favor code that enables automatic or passive identification so as to enhance compliance with the law. On the other hand, online privacy is a major concern of most Americans. For example, the Child Online Privacy Protection Act[190] mandates that online commercial sites that collect information about children accessing the sites keep this information private. The problem with these conflicting norms is that code enabling passive identification could be used for many purposes. It would be publicly available (or at least available for sale) to other sites, which could use this code for marketing, surveillance, research, or any other purpose. As a result, society is forced to choose between these conflicting norms.

How should the Internet and the law respond to these market forces and ambivalent social norms regarding passive-identification code? Because passive identification is beneficial to the market and protects at least one social norm, it is likely that code will develop in that direction and that all Internet users will suffer a significant loss of privacy.

B. Problems with Passive-Identification Code and Creation of a Free- Speech Zone

Existing caselaw might enable the Court to approve greater regulation of Internet speech if technology allowed simple and automatic age and geographic identification of website visitors.[191] Conversely, the Court might prefer a system that places at least some of the burden on receivers to avert their eyes.[192]

There are two primary problems with an Internet permeated by passive-identification code. First, privacy is a major concern of most Americans. As a result, if faced with the likelihood of being identified as receiving controversial, but constitutionally protected, speech, some individuals will choose not to receive it. This reluctance would extend to communications that are considered obscene or indecent in certain localities, even if legal in the receiver's jurisdiction. It would also extend to sites containing controversial political or social views. The fact that a website visitor might not have to input information actively does not change the result of being identified; it is the loss of anonymity, rather than the means of identification, that creates the problem. Consequently, passive-identification code will chill Internet speech.

---

190. *See generally* 15 U.S.C. §§ 6501-6506.

191. *See* Reno v. ACLU, 521 U.S. 844, 879 (1997).

192. *See* United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813 (2000); Cohen v. California, 403 U.S. 15, 21 (1971).

The widespread implementation of such a code would transform the Internet from a free-ranging mode of communication to primarily a commercial outlet. If people do not access controversial speech for fear of being identified, many websites that post such speech will cease to operate, leaving mostly commercial sites. Cyberspace will turn into just another shopping area.

To avoid such a result, the better approach to government regulation is to assign some responsibility to the receivers of speech for self-protection. There is no right to be free from offense; there is no law against being shocked. In fact, one of the benefits of free speech is that it may shock people into action. The rule is that those who find speech offensive should avert their eyes, close their ears, or speak their opinions.[193]

Even when the goal is to protect children, it is not the government's role to act as a parent. The government's role is merely to *help* parents shield their children from indecency. Parents are in the best position to avert the eyes of their children. Instead of imposing or encouraging architectural changes in the Internet that will chill protected speech, the Court should encourage listeners and parents to help themselves. Consequently, courts should continue to strike down laws that force senders of speech to identify their audience because such regimes are not the least restrictive means of regulating speech.

C. Helping Listeners Help Themselves: A Theoretical Model For Regulating Obscenity and Indecency on the Internet

Professors Lawrence Lessig and Paul Resnick recognize the dilemma facing the distributors and receivers of Internet communications that might be considered indecent.[194] These authors hypothesize that no party has enough information to determine whether blocking a transaction is appropriate. Therefore, the law must create an incentive for parties to provide that information.[195] Lessig and Resnick analyze two rules that would create such an incentive. The first would impose liability on the distributor if he or she enters into a transaction without indicators that it is legal, and the transaction later turns out to be illegal (the transaction is "prohibited unless permitted").[196] The second rule would impose liability on the distributor only if there are indicators that the transaction is illegal and it later turns out to be illegal (the "permitted unless

193. *Playboy*, 529 U.S. at 813-14.

194. Lessig & Resnick, *supra* note 3, at 403.

195. *Id.* at 401.

196. *Id.* at 402.

prohibited" rule).[197] Problems arise under both rules when there is uncertainty about the speech's content or the recipient's identity. The first rule is overbroad, and the second is ineffective because there is no incentive to discover the information needed.[198] Accordingly, these authors focus on changes in the architecture of the Internet that might reduce uncertainty.[199]

Lessig and Resnick propose a model regulation controlling child access to indecent material online.[200] The proposal responds to the imperfect-information problem — the inability to identify the age or jurisdiction of the receiver — with a limited form of passive identification. Rather than identifying all Internet users, the proposed regime requires self-identification only of children, and website operators would be required to block access only to those potential visitors.[201] Specifically, parents would use a tamper-resistant "kids-mode" browser that signals to servers that the user is a minor. The server hosting the sender's speech would detect and block a user identified as a child and would purge any identification data collected about the user except the data required to process user requests.[202] The authors argue that such a browser is available since browser–server communication already includes the browser type, the browser's IP address, and other useful information.[203] The model statute imposes minimal burdens on servers because they would be required only to identify whether the user is a child. According to the authors, such a burden would be trivial given the information that servers already collect from browsers.[204] In addition, all a parent would need to do is enable the kids-mode browsing. This burden is not as heavy as purchasing blocking software.[205]

Lessig and Resnick convincingly argue that such a regulation is superior to the CDA and COPA. First, it is less burdensome to signal that a user is a child than to signal that a user is an adult because there is no need to verify the signal.[206] Second, the regulation would burden fewer people because only

197. *Id.*

198. *Id.* at 403.

199. *Id.*

200. *Id.* at 416.

201. *Id.*

202. *Id.* at 416-17.

203. *Id.*

204. *Id.* at 417.

205. *Id.*

206. *Id.*

parents would need to take affirmative steps, rather than all adults who want full access to the Web.[207] Third, this regime is cheaper than blocking software.[208] Fourth, it places lower costs on senders and software manufacturers than does COPA.[209] Fifth, it is less invasive of users' privacy because instead of forcing adults to reveal their age through a verification service, the only information that would change hands is that the user is a child.[210] Sixth, the regime is less costly than an adult-identification system.[211] Finally, the regime would provide an easy way for schools to control Internet access.[212]

Another technological development that would place more responsibility on the receiver of Internet speech is a system in which Internet speakers would tag their speech as potentially indecent. Indeed, the Court hinted at this solution in *Reno I*.[213] Once in place, such a regulation would encourage parents or other Internet users to buy browsers sensitive to that tagging.[214] This sort of system balances the interests of speakers and receivers better than the use of passive-identification code. Such a law would protect the privacy interests of adults seeking access to sexually explicit or otherwise controversial speech, while ensuring that this material does not reach children whose parents, by purchasing browsers, have deemed it improper.

Such a tagging system could also be adapted to the problem of the differing standards for obscenity. Obscenity is unprotected, but the varying levels of "unprotection" create a problem for speakers who cannot identify what level of protection applies to specific audience members. Courts appear willing to hold distributors of obscenity liable in the jurisdiction of distribution, despite the boundlessness of the Internet. In the future, courts should take into account the speakers' efforts to notify receivers of the content of their sites and to dissuade users from accessing sites that are illegal in a given jurisdiction.

---

207. *Id.* at 419-20.

208. *Id.* at 420.

209. *Id.*

210. *Id.*

211. *Id.* at 420-21.

212. *Id.*

213. *See Reno I*, 521 U.S. at 887.

214. Lessig & Resnick, *supra* note 3, at 416-22.

VI. CONCLUSION

The Supreme Court's balancing of free-speech rights against the problems of obscenity and indecency were generated in the physical world, where it is possible to follow legal standards in specific geographic locations. It is unfair, however, to impose on Internet speakers regulations that turn on the content of unforeseeable "community standards." While a magazine seller knows where it is distributing magazines and can decide not to distribute them in certain states, a website operator lacks this crucial information and has no effective means of targeting specific locales. The lack of a physical connection between Internet speaker and Internet receiver creates a knowledge gap that only technology can bridge.

Solutions that bridge the gap by violating the privacy interests of all Internet users resemble unconstitutional indecency rules — they burn the house to roast the pig. The Court should continue to reject such rules as overbroad. Furthermore, legislators should adopt rules that create an incentive to develop a more limited and specific kind of identification code. Where the object is to protect children, parents should have access to browsers that can identify an Internet user as a child. Where the object is to protect a community from speech that is considered obscene under local standards, a website operator should be required only to warn users that the website may include content that is considered obscene in some communities. If the free-speech and privacy rights of all citizens are to be protected, then adults who find some speech offensive must take responsibility for averting their eyes and those of their children.