Zoning the Internet: A New Approach to Protecting Children Online

Cheryl B. Preston[*]

I. INTRODUCTION

Some movements generate a great deal of energy but seem to get no closer to their goal. The fight to save children and teens from Internet pornography has been one such endeavor. Weeks and years, impressive fortunes, and promising political careers have been consumed with good faith efforts to address this pressing problem. Statutes are drafted, passed, and litigated. Courts struggle to frame a proper test. The Supreme Court splits in pluralities. Statutes fail. All the while, academics, lawyers, and legislators churn arguments and ideas. Still, the problem grows. Pornographers find new and ingenious ways to circumvent filters, attract new categories of viewers, and build economic and political support. The number of sexually explicit Web pages multiplies. Younger and younger children learn to use the computer. Cheaper and smaller devices are engineered to be Web-enabled but not filtered. Unfiltered, unsecured WiFi hotspots pop up everywhere. In short, a generation of tech-savvy children is being exposed to sexually explicit material that is not age-appropriate, that they cannot fully process, and that they lack the judgment and experience to contextualize.

As Internet pornography metastasizes at an ever more alarming rate, many, like Justice Stevens in his concurring opinion in *Ashcroft v. ACLU* (*Ashcroft III*), express "a growing sense of unease" about any regulation of speech on the Internet.[1] In fact, the track record of prior legislative schemes in the courts suggests that no legal

* Edwin M. Thomas Professor of Law, J. Reuben Clark Law School, Brigham Young University; Visiting Professor of Law, S.J. Quinney College of Law, University of Utah; Board of Advisors, CP80.org, a non-profit foundation. I thank the following for their excellent comments on earlier drafts, their research and editing help, and their technology experience: Debra Peck, Christopher Reed, Kathleen Cannon, Jessica Andrew, Chad Staheli, Chad Worthen, Aaron Harris, Marin Bradshaw, Daniel Adlong, Michael Jensen, Scott Hilton, Galen Fletcher, and the team at CP80.org.

1. *See Ashcroft III*, 542 U.S. 656, 675 (2004) (Stevens, J., concurring).

mechanism for restricting children's access to Internet pornography will survive constitutional review. And, indeed, if approached again as an Internet-wide, transaction-based restriction, further attempts are likely doomed. The law, or East Coast Code as characterized by Larry Lessig,[2] seems hopeless as a means of addressing speech on the Internet.

Rather than give up in despair or pretend that any teen with a decent public education cannot bypass a filter, it is time to step back from failed patterns of government regulation and consider how Internet architecture can be harnessed to create an environment where government regulation can be effective but not unreasonably burdensome.

This Article proposes a solution that engages programming and technology, or West Coast Code,[3] in refocusing the point of regulation of Internet pornography, thereby reducing the burden of regulation on speech and increasing the ability to achieve constitutionally recognized governmental objectives. Part II briefly examines previous congressional attempts to restrict children's access to Internet pornography and the judicial responses. Part III explains the Internet Community Ports Concept, which relies on technology to zone Internet ports. Part IV then describes the Internet Community Ports Act (ICPA), which supports and enforces the zoning divisions. Thus, working together West Coast Code and East Coast Code can create safe places for children and families on the Internet. Part V responds to the issues raised by Professor Dawn Nunziato with respect to ICPA.[4] Finally, Part VI concludes by explaining how this two-pronged solution provides a constitutionally acceptable solution to the problem of underage access to Internet pornography.

2. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, at 72 (2006). In the Internet context, East Coast Code is a constraint on the Internet caused by law as enacted and enforced by Congress and the Supreme Court on the East Coast. West Coast Code is a constraint on the Internet caused by the technological architecture and software written and applied by geeks who are at least stereotypically identified with Silicon Valley, or the West Coast.

3. *See id.*

4. *See* Dawn C. Nunziato, *Technology and Pornography*, 2007 BYU L. REV. 1535, 1571–84.

II. LEARNING FROM THE PAST: EXAMINING PRIOR LEGISLATIVE SCHEMES

Congress has adopted two broad regulations aimed at protecting children from Internet pornography: the Communications Decency Act (CDA)[5] in 1996 and the Child Online Protection Act (COPA)[6] in 1998. The courts have effectively barred the application of both.

A. The Communications Decency Act of 1996

In perhaps a panicked response to the astonishing growth of pornography on the newly available Internet, Congress passed the poorly conceived CDA.[7] The CDA prohibited (1) knowingly transmitting "obscene or indecent messages to any recipient under 18 years of age," and (2) "knowing[ly] sending or displaying . . . patently offensive messages in a manner that is available to a person under 18 years of age" over the Internet.[8] Under the statute, a Web publisher who violated these provisions could be fined, imprisoned, or both.[9] Additionally, the CDA provided defenses against prosecution, including "tak[ing] . . . reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in [the CDA]" or "restrict[ing] access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number."[10]

Immediately after the CDA was signed into law, it was challenged on constitutional grounds.[11] In *ACLU v. Reno*,[12] a three-

5. 47 U.S.C. § 223 (2000). For a more detailed discussion of the CDA and COPA, see Nunziato, *supra* note 4, at 1544–55, 1564–70.

6. 47 U.S.C. § 231 (2000).

7. 47 U.S.C. § 223. Larry Lessig describes the CDA as a "law of extraordinary stupidity[;] [it] practically impaled itself on the First Amendment." LESSIG, *supra* note 2, at 249; *see also* Cheryl B. Preston, *The Internet and Pornography: What if Congress and the Supreme Court Had Been Comprised of Techies in 1995–1997?* (forthcoming in 2008 in MICH. ST. L. REV.) (on file with author).

8. Reno v. ACLU (*Reno I*), 521 U.S. 844, 859–60 (1997) (declaring unconstitutional 47 U.S.C. § 223(d) and a portion of 47 U.S.C. § 223(a)). The section that protects private actors, such as Internet service providers, from suit based on blocking or screening offensive online material is still in effect. *See* 47 U.S.C. § 230 (2000).

9. *See* 47 U.S.C. § 223(d).

10. *Id.* § 223(e)(5)(A)–(B).

11. *See* ACLU v. Reno, 929 F. Supp. 824, 826 (E.D. Pa. 1996).

12. *Id.*

judge district court panel enjoined the government from enforcing the CDA. In response, the government directly appealed to the Supreme Court.[13]

The Supreme Court struck down the Internet pornography provisions of the CDA in *Reno I*,[14] finding that the Act was a "content-based blanket restriction on speech" subject to strict scrutiny and thus could not be analyzed under intermediate scrutiny as a content-neutral "time, place, and manner regulation."[15] The Court also found that the language restricting speech in "the CDA lack[ed] the precision that the First Amendment requires when a statute regulates the content of speech."[16] Because of this vagueness, the Court held that "the CDA effectively suppresse[d] a large amount of speech that adults have a constitutional right to receive and to address to one another" and, as such, was not narrowly tailored to achieve the government's interest in protecting children from Internet pornography.[17] Additionally, the Court held that the CDA was not the least restrictive means to achieve the government's compelling interest of protecting minors.[18]

B. The Child Online Protection Act of 1998

In the aftermath of the CDA, Congress, recognizing the continuing problem of children's access to Internet pornography, crafted another statute to address the flaws so apparent in the CDA. Congress' efforts resulted in the passage of COPA in 1998.[19] COPA prohibits Web publishers with "commercial purposes" from knowingly making available on the Web material "harmful to minors."[20] Congress intended COPA to cover adult material that does not qualify under the narrowly applied definition of "obscenity" from *Miller v. California*,[21] which has no First Amendment

13. *See* Reno v. ACLU, 519 U.S. 1025 (1996) (mem.) (noting probable jurisdiction).

14. *Reno I*, 521 U.S. 844, 844, 885 (1997).

15. *Id.* at 868 (citation omitted).

16. *Id.* at 874.

17. *Id.*

18. *See id.* at 879.

19. COPA, 47 U.S.C. § 231 (2000).

20. *Id.* § 231(a)(1).

21. 413 U.S. 15, 24 (1972) ("The basic guidelines for the trier of fact must be: (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or

protection. COPA includes a definition of material "harmful to minors" built on the framework of the "obscenity" definition from *Miller*,[22] but it changes the focus to measure the impact and value of the material against a standard of a person under age seventeen.[23] The COPA definition of "material harmful to minors" is:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—
>
> (A) 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;
>
> (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 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.[24]

Violators of COPA face up to six months in prison, a $50,000 fine, or both for each violation.[25] However, COPA provides a defense to Web publishers who make a good faith effort to restrict

---

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.") (internal citations omitted). By 1994, the courts were applying this definition narrowly. *See, e.g.*, Jenkins v. Georgia, 418 U.S. 153, 160–61 (1974). In *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007), the court included two factual findings that reflect how difficult it has been to prosecute obscenity offenses:

> From 2000 to 2005, [the Justice Department] initiated fewer than 20 prosecutions for obscenity which did not also accompany charges of child pornography, travel in interstate commence to engage in sex with a minor, or attempting to transfer obscene material to a minor . . .[;]
>
> . . . [In addition, t]here have been fewer than 10 prosecutions for obscenity which did not also accompany charges of child pornography, travel in interstate commerce to engage in sex with a minor, or attempting to transfer obscene material to a minor since 2005.

Id. at 799.

22. *See Miller*, 413 U.S. at 24.
23. *See* 47 U.S.C. § 231.
24. *Id.* § 231(e)(6).
25. *See id.* § 231(a)(2)–(3).

minors from accessing "material that is harmful to minors—(A) by requiring 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."[26]

A suit challenging COPA was promptly filed.[27] In *Reno II*, the court in the Eastern District of Pennsylvania enjoined the enforcement of COPA.[28] On appeal, in *ACLU v. Reno* (*Reno III*),[29] the Third Circuit affirmed the district court's injunction, ruling that COPA's use of "contemporary community standards" to define "material harmful to minors" is unconstitutionally broad.[30] The Third Circuit reasoned that, unlike other outlets such as the mail or the telephone, the Internet could not be geographically constrained—that is, information published on the Internet could not be directed to specific communities.[31] The court stated that because people who publish information on the Internet cannot control where that information goes, the use of contemporary community standards would require Web publishers "of material that may be harmful to minors [to] 'comply with the regulation imposed by the State with the most stringent standard or [entirely] forego Internet communication of the message that might or might not subject [the publisher] to prosecution.'"[32] The Third Circuit concluded that this restriction would deprive adults of their constitutional right to view such materials.[33]

On appeal, in *Ashcroft v. ACLU* (*Ashcroft I*), the Supreme Court vacated the judgment in *Reno III*, ruling that the use of contemporary community standards to define what is harmful to minors did not, "by itself," make COPA unconstitutional.[34] However, the Court remanded the case to determine if COPA passed strict scrutiny on other grounds.[35]

26. *Id.* § 231(c)(1)–(2).
27. ACLU v. Reno (*Reno II*), 31 F. Supp. 2d 473, 499 (E.D. Pa. 1999).
28. *Id.*
29. 217 F.3d 162 (3d Cir. 2000).
30. *Id.* at 173–74.
31. *See id.* at 176.
32. *Id.* (quoting Am. Library Ass'n v. Pataki, 969 F. Supp. 160, 183 (S.D.N.Y. 1997)).
33. *See id.* at 177.
34. *Ashcroft I*, 535 U.S. 564, 585–86 (2002).
35. *See id.*

On remand, in *Ashcroft v. ACLU* (*Ashcroft II*), the Third Circuit again affirmed the district court's injunction because, after applying strict scrutiny to other aspects of COPA, the court still found it to be unconstitutional.[36] The court held that COPA is not "narrowly tailored" to protecting minors because the statute's definitions of terms like "'material that is harmful to minors'" and "'commercial purposes'" would prohibit "a wide range of protected expression."[37] The court also found that COPA is unconstitutionally overbroad.[38] Furthermore, the court found that COPA does not "employ the 'least restrictive means' to effect the Government's compelling interest" because other means of protecting children from pornography, such as filters, are available.[39]

COPA was again sent to the Supreme Court.[40] The Court's plurality ruling on appeal did not address the alleged overbreadth of COPA.[41] However, after subjecting COPA to strict scrutiny, the Court found that the government had not met its burden of proof in showing that less restrictive alternatives, such as filters, would not achieve the government objective as effectively as the new statutory regime.[42] The case was then remanded back to the district court to determine whether filters offer sufficient protection for children against Internet pornography, and, if not, whether other grounds exist for finding COPA unconstitutional.[43]

On remand in *ACLU v. Gonzales*, Judge Reed of the Eastern District of Pennsylvania issued a permanent injunction against the enforcement of COPA, ruling first that COPA is not narrowly tailored.[44] In making this determination, the court found that COPA is both over- and under-inclusive because it prohibits more speech than necessary and fails to block a significant amount of sexually explicit Internet material originating from outside of the United States.[45]

36. *Ashcroft II*, 322 F.3d 240, 243 (2003).
37. *Id*. at 253, 256–57 (quoting 47 U.S.C. § 231 (2000)).
38. *See id*. at 266–67.
39. *Id*. at 261.
40. *Ashcroft III*, 542 U.S. 656, 656 (2004).
41. *See id*. at 657.
42. *See id*. at 673.
43. *See id*. at 672–73.
44. ACLU v. Gonzales, 478 F. Supp. 2d 775, 810–13 (E.D. Pa. 2007).
45. *See id*. at 810.

The court also found that COPA is not the "least restrictive, most effective alternative in achieving the [government's] compelling interest" of protecting minors because "[filters] are at least as effective, and in fact, are more effective than COPA" in protecting children from sexually explicit material on the Web.[46] Additionally, the court found that COPA is vague in several of its definitions, thus making COPA overbroad.[47] The case has been appealed to the Third Circuit[48] and will likely return again to the Supreme Court; however, commentators find it unlikely that COPA will survive.[49]

C. Smaller Bites and Band-Aids: Legislation after COPA

Since COPA, Congress has passed other laws more limited in reach, with particular focus on the problem of children's access to Internet pornography. The first, the Child Internet Protection Act (CIPA), provides economic incentives to libraries that filter their computers so children cannot use them to access Internet pornography.[50] CIPA dictates that "a public library may not receive [certain kinds of] federal assistance to provide Internet access unless it installs software [1] to block images that constitute obscenity or child pornography, and [2] to prevent minors from obtaining access to material that is harmful to them."[51] Another law, the Truth in Domain Names Act (TDNA), makes it illegal to knowingly use a misleading domain name to "deceive a person into viewing material constituting obscenity" or to "deceive a minor into viewing material that is harmful to minors."[52]

46. *Id*. at 778, 815. The district court stated that "filters block sexually explicit foreign material on the Web, parents can customize filter settings depending on the ages of their children and what type of content they find objectionable, and filters are fairly easy to install and use." *Id*.

47. *Id*. at 816–20. Specifically, the court held that COPA is unconstitutionally vague because it 1) failed to define the scienter requirements; and 2) is unclear in its definitions of a) "communication for commercial purposes," b) "minor," and c) "as a whole." *Id*.

48. Third Circuit Docket Number 07-2539 (filed May 25, 2007).

49. For an opinion on the likely future of COPA, see Nunziato, *supra* note 4, at 1570 and Lawrence Lessig, *COPA is Struck Down*, LESSIG 2.0, Mar. 27, 2007, http://lessig.org/blog/2007/03/=copa_is_struck_down.html ("Another Philadelphia court has struck another effort by Congress to regulate 'harmful to minors' speech. . . . No surprise. Though it has taken almost a decade, it is the right answer given the flaws in the statute.").

50. CIPA, Pub. L. No. 106-554, 114 Stat. 2763, 2763A–335 (2000) (codified as amended in 20 U.S.C. § 9134(f), 47 U.S.C. § 254(h)(6)).

51. United States v. Am. Library Ass'n, 539 U.S. 194, 199 (2003).

52. TDNA, 18 U.S.C. § 2252B(a)–(b) (2006).

Although both of these laws are steps in the right direction and have not failed any constitutional challenges,[53] they do not provide a sufficient solution to the problem of underage access to Internet pornography. CIPA only requires Internet filters in libraries. Filters are often ineffective because they are easily circumvented,[54] and some libraries have chosen to forego the linked federal funding rather than comply. The TDNA may keep children from accessing pornography accidentally by misspelling a domain name, but it does not keep them from stumbling upon links of inappropriate material while searching innocent terms like "toys," "dolls," or "pets."[55] Furthermore, the TDNA does not address the issue of minors who intentionally seek Internet pornography or children who access harmful material on sites with quite accurate domain names.

Notwithstanding Congress's good intentions in passing the CDA, COPA, CIPA, and the TDNA, none of these laws adequately account for the unique characteristics of the Internet and their implications for First Amendment analysis. Current efforts focus on only two possible technological approaches to a solution. First, Congress has required all Web sites to interactively monitor access with each hit—an expensive and impractical process. Second, the Court is willing to rely on private filter companies to create software that appropriately distinguishes between innocent and harmful material, that keeps up with the rapid innovations in code and the massive influx of new Internet pages, and that creates a barrier sufficient to impede teenagers' explorative instincts. Neither approach promises to be an effective solution.

53. *See Am. Library Ass'n*, 539 U.S. at 214 (stating that CIPA did not cause libraries to violate the First Amendment and therefore was a legitimate exercise of congressional power). The constitutionality of the TDNA has not been challenged; at least one individual has been successfully prosecuted for violating it. *See* Christopher G. Clark, Note, *The Truth in Domain Names Act of 2003 and a Preventative Measure To Combat Typosquatting*, 89 CORNELL L. REV. 1476, 1512–13 (2004).

54. *See* Jacob A. Sosnay, *Regulating Minors' Access to Pornography via the Internet: What Options Does Congress Have Left?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 453, 480 (2005); DICK THORNBURG, NATIONAL RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET § 12.1.2 (2002).

55. *See* H.R. Rep. No. 105–775, at 10 (1998) (stating that one of the reasons Congress proposed COPA was the fact that children could find harmful materials by placing innocent terms in a search engine).

III. THE INTERNET COMMUNITY PORTS CONCEPT AND ACT

This section discusses a proposal that uses West Coast code and law, or East Coast Code, to address the problem of minors' access to Internet pornography. The core concept, consistent with regulation of hardcopy pornography, is zoning. In the virtual world, the Internet cannot be zoned geographically based on real world boundaries; however, it can be sorted horizontally, and each user can be given power to select which Internet ports or pathways are allowed into his or her home or business computer. The proposed solution discussed in this Article is sometimes called the Internet Community Ports Concept (the Ports Concept),[56] and the statute that creates the regulatory scheme to support it is ICPA. The text of ICPA and an explanation of its provisions appear in a companion article in this symposium issue.[57]

Internet users who want an Internet service governed by the real, geographical world's decency standards can purchase Internet service limited to those ports that are subject to regulation of pornographic content, or "Community Ports," as described below. Internet users who do nothing in response to this port separation, or who specifically request access to all ports, will continue to receive all available ports. The designation and separation of ports will be completely transparent to these users, whose Internet experience will not change in any way. However, Internet users who affirmatively request only Community Port access may then enter cyberspace with some assurance that the standards enforced in the real world will apply in the virtual space they access through their computers.

Fully understanding this Article's proposed solution depends on at least a basic level knowledge of how the Internet operates, and in particular, how users browse the Internet by looking at and requesting information from Web page publishers. The technical explanation of how this works with ports and packets follows in the next section.[58] For purposes of an overview explanation for those with little exposure to the mechanics of Internet functioning,

56. The Ports Concept was devised by CP80 Foundation. For more information on the workings of this proposal, visit CP80 Solutions: Technology, http://www.cp80.org/solutions/technology (last visited Nov. 13, 2007).

57. *See* Cheryl B. Preston, *Making Family-friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L. REV. 1471 app.

58. *See infra* Part III.A.

perhaps the best (although technically flawed) analogy is to cable-television channels. With content organized into channels, a parent can choose to block access to Internet pornography just as easily as he or she blocks unwanted cable-television channels—by simply calling his or her cable provider and requesting that the unwanted channel (or in this case the Open Port channels) be shut off from the digital feed to his or her receiver.

Of course, there will be opposition to such an approach, just as there is opposition to geographical zoning, television decency standards, fences, no trespassing signs, nuisance laws, and other limitations on the ability of some to impose sexually explicit material on others. The Ports Concept permits the freedom of those who want to speak and hear constitutionally protected adult speech while it recognizes the equally legitimate interests of those who do not want pornographic material in their homes and businesses. Most importantly, the Ports Concept also protects the right of parents to determine the means and materials by which their children are educated.

A. Understanding the Internet

Over sixty-five thousand ports or channels for the transmission of information currently exist in cyberspace.[59] Most traffic now travels over ten to twenty of these ports.[60] The default, or primary, range includes port 80,[61] over which the vast majority of current Web traffic passes, port 25, over which most e-mail traffic currently passes,[62] and the secured socket layer, over which encrypted

59. *See* Internet Assigned Numbers Authority, Port Numbers, http://www.iana.org/assignments/port-numbers (last visited Nov. 13, 2007) (explaining the uses for the different numbered ports); *see also* CP80 Solutions: Technology, www.cp80.org/solutions/technology (last visited Nov. 13, 2007) (listing many such ports); AuditMyPC.com, http://www.auditmypc.com/freescan/readingroom/port_scan_fyi.asp (last visited Oct. 22, 2007) (stating that there are over 65,000 internet ports). *See generally* Wikipedia, List of TCP and UDP Port Numbers, http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (last visited Oct. 10, 2007).

60. *See* CP80, Solutions: Technology, www.cp80.org/solutions/technology (last visited Nov. 13, 2007).

61. *See* Symantec, How Visible is My Computer? (Apr. 7, 2006), http://www.symantec.com/norton/library/article.jsp?aid=visible_computer ("Each port has a number and is dedicated to a particular function. For example, most Web traffic passes through port number 80.").

62. *See id.* ("Emails travel through port 25.").

information, such as credit card numbers and personal information, passes. The government and military use a range of secured ports, and technology experts can redirect their Internet access to another range of ports designated by numbers. However, the vast majority of these ports are unused.

The Ports Concept assumes that ranges of ports could be assigned to different purposes. One port group would be designated as the general commercial range—the Ports Concept calls this range the Community Ports.[63] The standards for this range of ports would be similar to the standards now applicable in the real world for areas of public traffic, such as streets, busses, and malls.[64] Another range of ports would be designed as Open Ports.[65] Any legal content could be transmitted over Open Ports under the Ports Concept.[66] Internet Service Providers can easily sort the two types of ports with free software.[67]

In the broadest sense possible, the Internet is a massive knot of connected computers from around the globe.[68] The World Wide Web consists of numerous computer networks linked together.[69] Each computer[70] attempting to access the Internet must become linked with the general Web of networks.[71] Internet Service Providers (ISPs) facilitate this link by allowing users to connect to

63. *See* Preston, *supra* note 57, at 1476–77.

64. *See id.*

65. *See id.*

66. *See id.*

67. *See id.*

68. *See* Vinton G. Cerf, *Computer Networking: Global Infrastructure for the 21st Century*, U. WASH. COMPUTING RESEARCH ASS'N, http://www.cs.washington.edu/homes/lazowska/cra/networks.html (last visited Oct. 24, 2007); *see also* Jeff Tyson, *How Internet Infrastructure Works: A Network Example*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet-infrastructure2.htm (last visited Oct. 25, 2007) ("In this way, every computer on the Internet connects to every other.").

69. *See* Tyson, *supra* note 68.

70. In this section of the article, "computer" refers to any device able to transmit and receive information on the Internet. This may include palm devices, cellular phones, online game consoles, etc.

71. *See* Jeff Tyson, *How Internet Infrastructure Works: A Hierarchy of Networks*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet-infrastructure1.htm (last visited Oct. 24, 2007) ("Every computer . . . connected to the Internet is part of a network. . . . When you connect to your ISP, you become part of their network. The ISP may then connect to a larger network and become part of their network. The Internet is simply a network of networks.").

their networks, which in turn connect to the worldwide network.[72] Upon connection, each computer receives a unique identifying number (known as an Internet Protocol Address or IP Address).[73] This address functions much like a street address in that it gives a point of reference for sending or receiving information. No two computers share the same IP Address on this worldwide network.[74]

Once connected to the global network, information can be transferred between computers. Web browsing, e-mail, encrypted Web traffic, and file transfers are types of information transfers that take place on the Web. To facilitate efficiency, differing kinds of data transfers are assigned to separate Internet ports[75] in much the same

72. *See id.*

73. *See* Charles M. Kozierok, IP Overview and Key Operational Characteristics, TCP/IP Guide, http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm (last visited Dec. 21, 2007) (discussing Internet Protocols and their purpose as points of reference)

74. *See* Jeff Tyson, *How Internet Infrastructure Works: Internet Protocol: IP Addresses*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet-infrastructure5.htm (last visited Oct. 25, 2007) ("Every machine on the Internet has a unique identifying number, called an IP Address.").

75. *See* CP80, Solutions: Technology, *supra* note 60, at fig.4 (reproduced *infra*) (discussing how "the combination of protocols and ports allows other applications using different protocols and ports to utilize network resources without conflicting or interfering with each other");

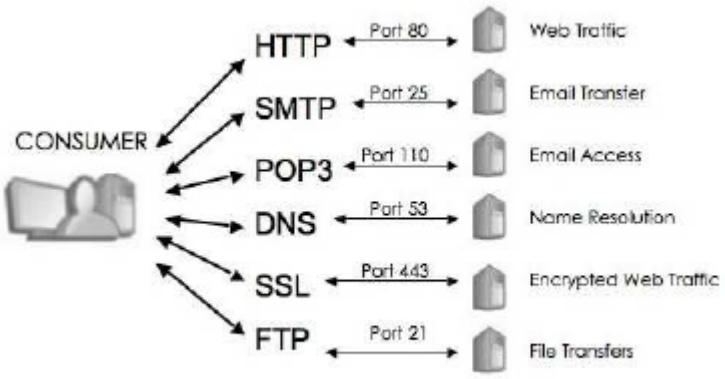


Fig. 4

see also Jeff Tyson, *How the Internet Infrastructure Works: Ports*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet-infrastructure10.htm (last visited Oct. 25,

way that different cable television stations are assigned to separate cable channels. Currently, however, Internet ports categorize differently than cable channels in a variety of ways. Internet ports categorize largely according to function—e-mailing and browsing, for example—while cable channels categorize according to pre-selected programming content. Nonetheless, the technology exists to leverage Internet ports to categorize data according to both function and content.

When a user browses the Internet by clicking on a link or entering a Web site, the user's computer sends a request to and receives a response from the targeted Web site through the intermediary ISP.[76] Port numbers facilitate this sending and receiving of information. When a request is sent to a computer, the Internet Protocol (IP) process determines the appropriate application to use based on the port number within the request. The protocol allows the computer to open, read, and respond to the request appropriately.[77] When a computer sends a request to an ISP, the ISP uses an IP system to determine the appropriate applications to process the request.[78]

The IP system can be thought of as a sorting mechanism for linking up the correct application for processing information. Because each port contains a certain type of information, the IP process currently makes this determination based on the port number used for the request.[79] For example, typical Web browsing uses the Hypertext Transfer Protocol (HTTP) to send and receive virtual packets. Because Web browsing uses HTTP, Web browsing

2007) ("Any server machine makes its services available using numbered ports—one for each service that is available on the server.")

76. *See* Charles M. Kozierok, HTTP Proxy Servers and Proxying, TCP/IP Guide, http://www.tcpipguide.com/free/t_HTTPProxyServersandProxying.htm (last visited Dec. 21, 2007) (describing an ISP's function as an intermediary, requesting information and receiving responses).

77. *See* Tyson, *supra* note 74 ("A protocol is the pre-defined way that someone who wants to use a service talks with that service.").

78. For a basic explanation of such applications, see Charles M. Kozierok, Protocols: What Are They, Anyway?, TCP/IP Guide, http://www.tcpipguide.com/free/t_ProtocolsWhatAreTheyAnyway.htm (last visited Dec. 21, 2007).

79. *See* Charles M. Kozierok, TCP/IP Application Assignments and Server Port Number Ranges, TCP/IP Guide, http://www.tcpipguide.com/free/t_TCPIPApplicationAssignmentsandServerPortNumberRang.htm (last visited Dec. 21, 2007) (explaining that, in order to avoid chaos, certain port numbers are reserved for certain applications).

content is now sent via port 80. Electronic mail transfers use the Simple Mail Transfer Protocol (SMTP) and are assigned to port 25. The combination of protocols and ports allows other applications using different protocols and ports to be on the system of fiber optic cables that form the infrastructure of the Internet without conflicting or interfering with each other.[80]

B. Creating Community Ports

While there are over 65,000 available ports on the Internet,[81] only a small fraction are being used for general Internet traffic. As mentioned above, currently all standard Web content uses the same port for transmission—port 80.[82] Whether it is sport scores, financial information, news, children's programming, or pornography on the Web, the information packets are transmitted over port 80. Although there is plenty of capacity on port 80 for this kind of browsing, nothing requires that all of this information be conducted over a single port.[83] A plain language analogy described in the New York Daily News, although not technically precise, is useful.[84] Imagine having every possible cable program crammed simultaneously onto a single cable channel and subject to being sorted and selected by the user of the cable receiver in the home. Would we tolerate a single cable channel broadcasting critical research and health information, children's cartoons, and sexually explicit programming? Yet this is exactly what happens on the Internet.

Fortunately, however, just as there are different cable channels to categorize and organize the different types of programming available to cable consumers, current technology exists that allows for the same effect of zoning or classification of Internet content. Thus, with Internet content zoned into different Internet ports, consumers can easily and definitively choose which channels (in this case, ports) they

80. *See generally* CP80, Solutions: Technology, *supra* note 60 (providing a general technical overview of how the Internet and the solution proposed by this Article work).

81. *See* Internet Assigned Numbers Authority, *supra* note 59.

82. *See* Kozierok, *supra* note 79 (describing port 80 as the default port).

83. *See id.* (explaining that users may explicitly direct the Web browser to use a port other than the default port 80).

84. Adam Nichols, *Cable Porn Gaffe: The Full Mickey!*, N.Y. DAILY NEWS, May 2, 2007, http://www.nydailynews.com/news/2007/05/02/2007-05-02_cable_porn_gaffe_the_full_mickey-1.html.

want to access or block through their Internet service in their home or office, just as they do with cable television. Equipment attached or wirelessly linked to a Community Ports-only service will never receive packets from any Open Port. Access is impossible, rather than subject to imperfect computer-installed filters, which users can hack past, circumvent, or disable, and which must be regularly updated and monitored.

Free programming code divides content by machine-readable port numbers at the Web server level through ISPs. The divisions would separate content into two basic categories of port ranges, in addition to those ports that are now separated for governmental, military, and other uses. More sophisticated divisions could be implemented upon increased consumer demand and technological innovation. The initial categories are "Community Ports" and "Open Ports." ICPA imposes civil and criminal penalties, depending on the degree and nature of the violation, on those who Post or place content on a Community Port that is Obscene, Harmful to Minors, or consists of Child pornography.[85] Open Ports may transmit all other legal content, including adult material that fits the definition of Harmful to Minors.

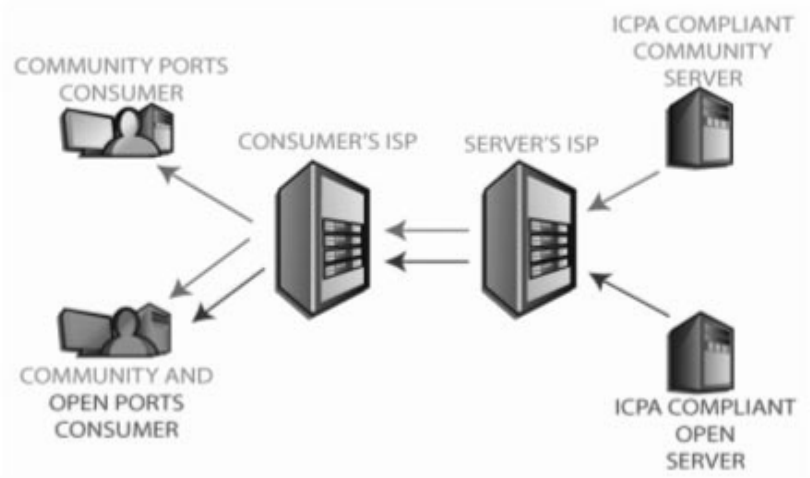
This proposed zoning of content regulates the means of delivery of Internet pornography by separating it rather than blocking it. All constitutionally protected content is available to adults who take no action, without any change in its appearance or method of delivery. The process will be entirely transparent to Internet users with a service that includes Open Ports. But, with content organized into ports, other consumers can then choose to opt out of the Open Ports and to receive only the Community Ports. Switching between ports takes place transparently to the consumer and can occur between any designated ports with no impact to network performance and no increased cost.[86]

85. *See* Preston, *supra* note 57, at 1471 app. § III(8)–(9).

86. This type of transparent switching takes place all the time. *See infra* for an illustration. For example, "a consumer shopping online at a Web site such as Amazon.com browses existing inventory over port 80. When a purchase is made, the transaction occurs securely via port 443. The consumer then returns to port 80 to continue browsing without ever realizing that the port switch had occurred." CP80, Solutions: Technology, *supra* note 60. For a list of well-known port numbers already in use, see Charles M. Kozierok, Common TCP/IP Applications and Assigned Well-Known and Registered Port Numbers, TCP/IP Guide, http://www.tcpipguide.com/free/t_CommonTCPIPApplicationsandAssignedWellKnownandRegi-2.htm.

The benefits of Internet zoning are not entirely without cost. Compliance with the division of content imposes a de minimis burden on Internet providers (who need only add the free programming code that effectuates the customer's purchase choice) and on those Web page publishers who wish to post adult content (who need only add free programming code to their servers once). Publishers of mature content are certainly not "banished" to the Open Ports. If a Web site contains both mature content and content appropriate for minors, the Web publisher can easily configure its server to transmit the information packets containing adult content over Open Ports, and the remainder may continue to be transmitted over Community Ports. An Internet user with only Community Port service will open a page with content acceptable for the entire family, but that has, rather than immediately visible adult images or text, links to such content. When such a user attempts to follow a link to the adult content, the computer screen will indicate that the page requested is not available. The Internet user whose service includes both categories of ports will be able to follow the link without delay. Thus, publishers of mature content can still publish the universally acceptable material on Community Ports with simple "click" links to the adult material.

Additionally, setup costs for Internet providers and publishers are minimal. The proposed zoning of Internet content regulates delivery of Internet pornography by separation rather than blocking. This



separation takes place at the publisher's server when it serves material to a particular port depending on its content. Thus, Web publishers who wish to post adult content may comply with the regulation by configuring their servers with a simple code, like a zip code, that directs such content to Open Ports. This is an easy Web server setup procedure and is often accomplished with less than ten lines of additional configuration.[87] This computer code is unseen and has no impact on the content of the material served. Indeed, Web publishers will suffer little to no additional costs associated with this proposed zoning of the Internet.

In sum, this concept of Community and Open Ports is a highly effective solution to the problems surrounding children's access to harmful Internet content. This solution is superior to prior regulatory attempts because (1) users are given the choice to "opt in" to the Community Ports program, (2) existing Internet providers and Web page publishers are only minimally burdened, and (3) establishing the electronic framework for the system is very inexpensive, causes no delays, and makes no change in the visible content or the meaning conveyed by the Internet speech.

C. Crafting Appropriate Legislation

In addition to the technological structures that make user choice possible, the solution to Internet pornography also requires legislation to enforce compliance with the Community Port criteria.[88] Although such a law could take various forms, this Article assumes a statute similar to ICPA, which is described later in this symposium issue.[89] Significantly, this proposed law does not prevent an adult from publishing or viewing any legal pornographic content. Rather, it only requires that adult content be published to transmit over a Port option that not all Internet Users need allow onto their computers. Thus, this legislation preserves the choices made by consumers who opt for only a Community Port-delivered Internet service. A statute, such as ICPA, must be adopted at the federal level and establish penalties for Web publishers who violate the law by Transmitting content that is illegal on any Port or content that is Harmful to Minors on Community Ports.

87. *See* CP80, Solutions: Technology, *supra* note 60.

88. *See* Preston, *supra* note 57, at 1471 app.

89. *See id.*

Very briefly, the proposed statutory scheme of ICPA is as follows. First, ICPA contains numerous Congressional Findings regarding the need for the statute. Second, it asserts the offense: knowingly publishing content that is Child pornography, Obscene, or Harmful to Minors on Community Ports.[90] The statutory language also prohibits creating Proxy sites that enable Internet Users on a Community Port-only service to access Open Ports. Third, the statute allows for a consumer reporting scheme by which Internet Users who find prohibited content on Community Ports may notify the FCC (or other regulatory entity) of the violation,[91] much like the current reporting process for indecency on prime time, licensed television programming.[92] After this Notification, an administrative process may be commenced by the FCC or the complaining consumer.[93] Violation of a court order to cease posting certain content on a Community Port may support criminal penalties.

Under ICPA, private parties that receive prohibited Communications over a Community Port are also empowered to pursue civil remedies, with damages dependent on several factors, such as whether the violating Communication was Obscene or merely Harmful to Minors and whether the Communication was made for Commercial Purposes.[94] In addition, the statute contains rules regarding attorneys' fees, class actions, and punitive damages.[95]

The statute provides safe harbors from liability for ISPs, so long as the ISPs keep a record of those individuals to whom they have issued IP Addresses so that information identifying offending Web publishers can be obtained by court order.[96] The statute also requires Wireless Networks that broadcast an Open Port connection to use passwords or other reasonable methods to limit access to adult

90. *See* Preston, *supra* note 57, at 1471 app. § II(1).

91. *See id.* at § II(2).

92. The FCC currently accepts complaints by mail, e-mail, fax, or telephone; for more information and a flowchart explaining the complaint process, see How the FCC Resolves Obscenity /Indecency/Profanity Complaints, http://www.fcc.gov/eb/oip/flow.pdf (last visited Oct. 25, 2007).

93. *See* Preston, *supra* note 57, at 1471 app. § III(3).

94. *See id.* § III(8)(i).

95. *See id.* § III(8)(ii).

96. *See id.* § II(4).

content over their networks by strangers.[97] Finally, ICPA defines technical jargon and other critical terms, such as the standard for material that is "Harmful to Minors."[98] When referring to IPCA in this Article, the terms defined therein are capitalized.

IV. THE INTERNET COMMUNITY PORTS CONCEPT AND CONSTITUTIONAL SCRUTINY

In addition to implicating several compelling governmental interests, the Ports Concept shifts the constitutional analysis from an onerous and universal burden applicable to every Internet User to a regulation applicable only to those who opt in to the regulatory scheme, and a minimal routing requirement on those who choose to publish low-value pornographic speech. Unlike COPA, which burdens "everyone" by requiring all Internet users—adults and kids—to identify themselves before accessing Web pages that contain material Harmful to Minors,[99] under ICPA, only those who voluntarily opt in to a Community Ports plan face any restriction in accessing protected speech. Those who do not opt in to a

97. *See id.* § II(2).

98. The ICPA definition of an Internet communication that is "Harmful to Minors" generally comports with the definition for such material under COPA, with some additions explained in the Community Ports Concept later in this issue. The definition is as follows:

> [A]ny Communication that:
>
> i. the average adult, applying a contemporary national standard, would find, taking the Communication as a whole, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> ii. 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, or describes or depicts Sexually Explicit Conduct [as defined in 47 U.S.C. § 231(e)(6), which lists graphically the actions that constitute such Conduct for child pornography purposes]; and
>
> iii. taken as a whole, lacks serious literary, artistic, political, or scientific value for Minors.

Id. § V(22). ICPA also defines "Minor" as any person who is under seventeen years of age. The "under age seventeen" standard should be interpreted to mean that only those materials inappropriate for fifteen- and sixteen-year-olds are targeted. Although material that is suitable for sixteen- and fifteen-year-olds may not be suitable for a five-year-old, parents have much greater control over the activity of a five-year-old, and few five-year-olds are computer savvy enough to hack through a filter or creatively explore the Internet. The designation of a person under age seventeen is taken from Supreme Court language in *Ginsberg v. New York*, 390 U.S. 629, 631 (1968) and *Reno I*, 521 U.S. 844, 859 (1997).

99. *See* 47 U.S.C. 231(c)(1) (2000).

Community Port-only service (e.g., those who do nothing) keep the status quo and will observe no difference in their Internet experience. Thus, the Ports Concept and ICPA, which put discretion to opt into regulation in the hands of the speech recipient, are a much easier fit under the First Amendment's protections. Proponents of Internet pornography regulation need not conclude from past courtroom experiences with the CDA and COPA that such regulation can never survive even strict scrutiny.[100]

A. Compelling Governmental Interests

To survive strict scrutiny, a congressional enactment must be aimed at serving a compelling governmental interest.[101] The change to an opt-in recipient regulation allows ICPA to serve not only the compelling interest of protecting minors but also two other compelling interests recognized in constitutional analyses.[102] Although only a single compelling interest is necessary for strict scrutiny purposes, an act that may not be seen as the least-restrictive means of achieving one interest may indeed be the least-restrictive means of achieving another equally compelling interest.

ICPA serves three governmental objectives that the Supreme Court has upheld as compelling: (1) protecting children,[103] (2) protecting the right of parents to raise their children according to their parental desires,[104] and (3) protecting the right of property owners to be free from invasive speech.[105]

1. Protecting minors

Minors need the protection of society against Internet pornography. The law holds that "infants do not have the mental capacity and discretion to protect themselves from the artful designs of adults."[106] Thus, many kinds of legislation have been enacted to

100. *See supra* Part II.A–B.

101. *Ashcroft II*, 322 F.3d 240, 251 (2003) (citing Sable Comm. of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989)).

102. *See infra* Part IV.A.

103. *See infra* Part IV.A.1.

104. *See infra* Part IV.A.2.

105. *See infra* Part IV.A.3.

106. City of New York v. Stringfellow's of N.Y., Ltd., 684 N.Y.S.2d 544, 551 (App. Div. 1999).

protect minors from the dangers of the adult world and even from themselves. For instance, minors do not have the Second Amendment right to bear arms, and a state may require adults to carry the burden of protecting children from guns.[107] In Texas, a gun owner is criminally negligent if a child gains access to a readily dischargeable firearm and the gun owner failed to secure the firearm.[108] The gun owner is guilty of a class C misdemeanor, or, if a person is killed or seriously injured, a class A misdemeanor.[109]

States also prohibit selling liquor to minors,[110] alcohol consumption by minors,[111] employing minors during school hours or in hazardous work,[112] providing tobacco products to minors,[113] permitting minors to use tobacco in a place of business,[114] providing certain weapons to minors,[115] body piercing or tattooing minors,[116] and entering into contracts with minors.[117] In *Reno I*, the Supreme Court reaffirmed that "'there is a compelling interest in protecting the physical and psychological well-being of minors' which extend[s] to shielding them from indecent messages that are not obscene by adult standards."[118]

107. *See, e.g.*, CAL. CIV. CODE § 1714.3 (West 1998); FLA. STAT. ANN. § 790.17 (West 2007); UTAH CODE ANN. § 76-10-509.6, 509.7 (2004).

108. *See* TEX. PENAL CODE ANN. § 46.13 (Vernon 2003).

109. *See id.*

110. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 25602.1, 25658(a) (West 2007); N.Y. ALCO. BEV. CONT. LAW § 65(a) (McKinney 2000); UTAH CODE ANN. § 32A-12-203 (West 2004).

111. *See, e.g.*, CAL. BUS. & PROF. CODE § 25658(d) (West 2007); FLA. STAT. ANN. § 768.125 (West 2005); UTAH CODE ANN. § 32A-12-217 (West 2004).

112. *See, e.g.*, CAL. LAB. CODE §§ 1294.1, 1391 (West 2003); FLA. STAT. ANN. §§ 450.061, .141 (West 2003); N.Y. LAB. LAW § 143 (McKinney 2003); UTAH CODE ANN. §§ 34-23-201, -203, & -302 (West 2004).

113. *See, e.g.*, CAL. BUS. & PROF. CODE § 22951 (West 2007); CAL. HEALTH & SAFETY CODE §§ 118950, 104350 (West 2007); CAL. PENAL CODE § 308(a)(1) (West 2007); N.Y. PUB. HEALTH LAW § 1399-cc (McKinney 2007); UTAH CODE ANN. § 76-10-104 (West 2004).

114. *See, e.g.*, CAL. PENAL CODE § 308(2)(b) (West 2007); UTAH CODE ANN. § 76-10-103 (West 2004).

115. *See, e.g.*, CAL. PENAL CODE § 12072(a)(3)(A) (West 2007); N.Y. PENAL LAW § 265.16 (McKinney 2007); UTAH CODE ANN. § 76-10-509.5 (West 2004).

116. *See, e.g.*, CAL. PENAL CODE §§ 652(a), 653 (West 1999); FLA. STAT. ANN. §§ 381.0075(7), 877.04 (West 2000); N.Y. PENAL LAW § 260.21 (McKinney 2000); UTAH CODE ANN. § 76-10-2201 (West 2007).

117. *See, e.g.*, CAL. CIV. CODE § 1556 (West 1982); UTAH CODE ANN. § 15-2-2 (West 2004).

118. *Reno I*, 521 U.S. 844, 869 (1997) (quoting Sable Commc'ns, Inc. v. FCC, 492 U.S. 115, 126 (1989)); *see also* New York v. Ferber, 458 U.S. 747, 756–57 (1982).

The rationale for restricting the legal rights of, and demands on, minors is based in our social, cultural, and scientific understanding of adolescence. Adolescent brains are still developing and are not as well equipped as adult brains to weigh choices and exercise judgment.[119] Under the law, children are considered differently than adults because of the peculiar vulnerability of children; their inability to make critical decisions in an informed, mature manner; and the importance of the parental role in child rearing.[120]

> Infancy, since common-law times and most likely long before, is a legal disability and an infant, in the absence of evidence to the contrary, is universally considered to be lacking in judgment, since his or her normal condition is that of incompetency. In addition, an infant is deemed to lack the adult's knowledge of the probable consequences of his or her acts or omissions and the capacity to make effective use of such knowledge as he or she has. It is the policy of the law to look after the interests of infants, who are considered incapable of looking after their own affairs, to protect them from their own folly and improvidence, and to prevent adults from taking advantage of them.[121]

The law recognizes a governmental interest in protecting children, regardless of the responsibilities of parents. Supreme Court precedent continues to firmly support this interest. "While the supervision of children's [access to material] may best be left to their parents, the knowledge that parental control or guidance cannot always be provided and society's transcendent interest in protecting the welfare of children justify reasonable regulation of the sale of

> It is evident beyond the need for elaboration that a State's interest in "safeguarding the physical and psychological well-being of a minor" is "compelling." . . . Accordingly, we have sustained legislation aimed at protecting the physical and emotional well-being of youth even when the laws have operated in the sensitive area of constitutionally protected rights.

Id.

119. *See* PBS.org, Frontline, *Interview with Deborah Yurgelun-Todd*, http://www-c.pbs.org/wgbh/pages/frontline/shows/teenbrain/interviews/todd.html (last visited Jan. 31, 3008). Dr. Yurgelun-Todd, a Harvard Medical School Researcher explains that "one of the things that teenagers seem to do is to respond more strongly with gut response than they do with evaluating the consequences of what they are doing." *Id.*

120. *See id.*

121. City of New York v. Stringfellow's of N.Y., Ltd., 684 N.Y.S.2d 544, 550–51 (App. Div. 1999). In this case, an adult establishment attempted to skirt the city's zoning ordinances by allowing children to enter if they signed a waiver releasing the establishment from any liability for any damage caused to them by viewing uncovered female breasts. *Id.* at 550.

[pornographic] material to them."[122] Parents are entitled to "the support of laws" in maintaining an option for Internet access without pornography.[123]

In *Reno I*, the Court again rejected the idea that "'the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor.'"[124] The Court held instead that the state has an "independent interest in the well-being of its youth,"[125] which justifies regulating speech notwithstanding the responsibilities of parents.

2. Protecting the right of parents to decide

A second compelling governmental interest is also relevant to the discussion of regulating Internet pornography—that of parental rights in deciding how children learn. The Supreme Court has stated that the government has a compelling interest in supporting parents' authority to raise their children in the manner they see fit.[126] The government acts on behalf of parents, not in place of them. In *Ginsberg v. New York*, the Supreme Court considered the appeal of a defendant convicted of violating a New York statute prohibiting the sale of materials harmful to individuals under the age of seventeen. The Supreme Court declared, "[C]onstitutional interpretation has consistently recognized that the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society."[127] In *Prince v. Massachusetts*, the Court further added that it "is cardinal with us that the custody, care, and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder."[128]

Although in *Reno I* the Supreme Court distinguished the statute that was held constitutional in *Ginsberg* from the CDA, it did so not because the Court's views on parental rights had changed, but

122. People v. Kahan, 206 N.E.2d 333, 334 (N.Y. 1965) (Fuld, J., concurring).
123. S*ee* Ginsberg v. New York, 390 U.S. 629, 639 (1968).
124. *Reno I*, 521 U.S. 844, 865 (1997) (quoting *Ginsberg*, 390 U.S. at 636).
125. *Id*. (quoting *Ginsberg*, 390 U.S. at 640).
126. *See Ginsberg*, 390 U.S. at 639; Prince v. Massachusetts, 321 U.S. 158, 166 (1944).
127. *Ginsberg*, 390 U.S. at 639.
128. *Prince*, 321 U.S. at 166.

because the *Ginsberg* statute was more narrowly tailored than the CDA.[129] In fact, the Court reaffirmed that parents have claim to the authority "to direct the rearing of their children," stating again that this authority "is basic in the structure of our society."[130]

For example, the state respects parents' decisions regarding placing their children in private sectarian schools rather than public schools,[131] placing them in schools that teach in languages other than English,[132] and, at times, taking them out of school altogether.[133] "[P]arents should be the ones to choose whether to expose their children to certain people or ideas."[134] To their downfall, the CDA and COPA relied on the government to decide what content all Internet users may access.[135] Under the Ports Concept, however, the government does not decide what is acceptable on the Internet for everyone; instead, it allows users (and thus, parents) the option of choosing a pornography-free Internet and then supports that choice by providing a remedy when an outsider tries to override that choice by depositing unwanted material onto the user's computer screen.

Because the state respects parental authority, it must provide the "support of laws designed to aid [the] discharge of that responsibility."[136] Further, the state assists when "parental control or guidance cannot always be provided."[137] The government has a responsibility to protect the morals of children in a manner that does not impose its morality on children, but rather, that supports "the right of parents to deal with the morals of their children as they see fit."[138] Thus, a statute that gives to parents the power to control what Internet materials are accessible by their children in the home maximizes this governmental interest.

129. *See Reno I*, 521 U.S. at 865 ("In four important respects, the statute upheld in *Ginsberg* was narrower than the CDA.").

130. *Id*. at 865 (quoting *Ginsberg*, 390 U.S. at 639).

131. *See* Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925).

132. *See* Meyer v. Nebraska, 262 U.S. 390 (1923).

133. *See* Sch. Dist. of City of Grand Rapids v. Ball, 473 U.S. 373 (1985); Wisconsin v. Yoder, 406 U.S. 205 (1972).

134. Troxel v. Granville, 530 U.S. 57, 63 (2000) (quoting *In re* Custody of Smith, 969 P.2d 21, 31 (Wash. 1998)).

135. *See* 47 U.S.C. §§ 223, 231 (2000).

136. Ginsberg v. New York, 390 U.S. 629, 639 (1968).

137. *Id*. at 640 (quoting People v. Kahan, 206 N.E.2d 333, 334 (Fuld, J., concurring)).

138. *Id*. at 639–40 n.7 (quoting Louis Henkin, *Morals and the Constitution: The Sin of Obscenity*, 63 COLUM. L. REV. 391, 413 n.68 (1963)).

3. Protecting the privacy of property owners

A third compelling interest is also at stake. Courts recognize a substantial governmental interest in protecting the right to privacy in homes and other private domains. The Supreme Court insists that "unwilling listeners may be protected when within their own homes."[139] In *Hill v. Colorado* the Court reiterated: "The unwilling listener's interest in avoiding unwanted communication has been repeatedly identified" and protected.[140] Further, "[t]he right to avoid unwelcome speech has special force in the privacy of the home and its immediate surroundings."[141]

Recently, Congress enacted the Do-Not-Call Registry Act (the Registry),[142] a statute prohibiting commercial telemarketers from making unsolicited calls to households that have placed their telephone numbers on a government-maintained registry. Its purpose was to "protect residential telephone subscriber privacy rights."[143] When the constitutionality of the Registry was challenged in *Mainstream Marketing Services, Inc. v. FTC*,[144] the Tenth Circuit held that it was constitutional, stating, among other things, that the Registry "targets speech that invades the privacy of the home, a personal sanctuary that enjoys a unique status in our constitutional jurisprudence."[145] The Tenth Circuit went on to declare:

> One important aspect of residential privacy is protection of the unwilling listener. . . . [A] special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions. Thus, we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may protect this freedom.[146]

139. Frisby v. Schultz, 487 U.S. 474, 485 (1988). In this case, the Court emphasized the sanctity of the home as a refuge from unwanted speech and upheld a speech restriction on that basis. *Id.* at 484–85, 488.

140. Hill v. Colorado, 530 U.S. 703, 716 (2000).

141. *Id.* at 717 (citations omitted).

142. 15 U.S.C. § 1601 (2003).

143. 47 U.S.C. § 227(C)(1) (2005).

144. 358 F.3d 1228 (10th Cir. 2004), *cert. denied*, 543 U.S. 812 (2004).

145. *Id.* at 1233.

146. *Id.* at 1237–38 (quoting Frisby v. Schultz, 487 U.S. 474, 484–85 (1988)) (alteration in original).

The Supreme Court denied the petitioners' request for certiorari.[147]

With respect to a similar statute, Section 4009 of Title III of the Postal Revenue and Federal Salary Act of 1967 (the Pandering Mail Act),[148] the Supreme Court also discussed the state's interest in protecting the privacy of the home.[149] This legislation allows homeowners to request that their names and addresses be removed from the mailing list of any mailer from whom they have once received material that, based on the homeowners' discretion, is erotically arousing or sexually provocative.[150] In *Rowan v. U.S. Post Office Department*, the Supreme Court found that Congress's objective for enacting the Pandering Mail Act "was to protect minors and the privacy of homes from [sexually explicit] material."[151] The Court then recognized that, even if the Pandering Mail Act did impede the flow of valid ideas into a home, "no one has a right to press even 'good' ideas on an unwilling recipient."[152]

The Fifth Amendment guarantees the right to control property. Notwithstanding the First Amendment, owners may pick and choose whom they invite onto their purely private property.

> Although accommodations between the values protected by [the First, Fifth and Fourteenth] Amendments are sometimes necessary, and the courts properly have shown a special solicitude for the guarantees of the First Amendment, this Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.[153]

When invited guests exceed the limits of permitted conduct or speech imposed by the property owner, such guests become

147. Mainstream Mktg. Servs., Inc. v. FTC, 543 U.S. 812 (2004) (mem.).

148. Postal Revenue and Federal Salary Act of 1967, 39 U.S.C. § 3008 (2000).

149. Rowan v. U.S. Post Office Dep't., 397 U.S. 728, 730–40 (1970).

150. *See id.* at 730.

151. *Id.* at 732.

152. *Id.* at 738. Similarly, the Court found in a separate case that captive audiences driving or riding in streetcars should not be forced to view communications through "no choice or volition" of their own. Lehman v. Shaker Heights, 418 U.S. 298, 302 (1974) (quoting Packer Corp. v. Utah, 285 U.S. 105, 110 (1932)).

153. Lloyd Corp. v. Tanner, 407 U.S. 551, 568–69 (1971) (emphasis added); *see also* Cent. Hardware Co. v. NLRB, 407 U.S. 539, 547 (1972) ("Before an owner of private property can be subjected to the commands of the First and Fourteenth Amendments the privately owned property must assume to some significant degree the functional attributes of public property devoted to public use.").

trespassers and the state will assist the property owner with removing them.[154]

A similar right exists, of course, with respect to the private property of business owners. Employers are entitled to control their work environment. The Supreme Court held in *Cornelius v. NAACP Legal Defense and Educational Fund, Inc.*[155] that even

> the Government, as an employer, must have wide discretion and control over the management of its personnel and internal affairs." It follows that the Government has the right to exercise control over access to the federal workplace in order to avoid interruptions to the performance of the duties of its employees.[156]

The Supreme Court has also recognized that speech can be limited in a nonpublic forum, such as a workplace or a home,

> based on subject matter and speaker identity so long as the distinctions drawn are reasonable in light of the purpose served by the forum and are viewpoint neutral [in the political sense]. . . . [A] speaker may be excluded from a nonpublic forum if he wishes to address a topic not encompassed within the purpose of the forum or if he is not a member of the class of speakers for whose especial benefit the forum was created . . . .[157]

The Supreme Court's recent characterization of the Internet emphasizes its characteristics at the point of delivery rather than somewhere in the exchange of packets along the fiber optic root system.[158] The *United States v. American Libraries Ass'n* majority stated

> Internet access in public libraries is neither a "traditional" nor a "designated" public forum. . . . As Congress recognized, "[t]he Internet is simply another method for making information available

154. *See, e.g.*, Champlin v. Walker, 249 N.W.2d 839 (Iowa 1977) (finding that plaintiff who was a social guest at a friend's home was a trespasser when he went beyond the limits of his invitation).

155. 473 U.S. 788 (1985).

156. *Id.* at 805–06 (quoting Arnett v. Kennedy, 416 U.S. 134, 168 (1974) (Powell, J., concurring in part)) (other citations omitted).

157. *Id.* at 806.

158. *See* United States v. Am. Library Ass'n, 539 U.S. 194, 205–06 (2003). The Court did not subject the statute in *American Library Ass'n* to strict scrutiny, and the case is thus distinguishable on its holding. Nonetheless, the characterization of the Internet as a nonpublic forum based on its point of delivery is useful.

> in a school or library." It is "no more than a technological extension of the book stack."[159]

Thus, if the Internet access point in a public library is not a public forum and no more than an extension of a book stack, then the Internet available on a consumer's personal computer is, for constitutional purposes, no more than an extension of the books on the shelf in his or her home. Further, the Internet in a workplace is no more than an extension of the reading material an employer chooses to stock in the employee lounge.

ICPA affords a solution that protects children, parental choice, property rights, and the ability of adults who do not opt-in to the regulatory scheme to continue to access legal pornographic material.

B. Narrowly Tailored to Address Compelling Interests

In First Amendment jurisprudence, once a compelling governmental interest is established, the Court then determines if the statute in question is over- or under-inclusive.[160] To pass this strict scrutiny analysis, as proffered by the Supreme Court in *Ashcroft III*, any statute that regulates Internet speech must be narrowly tailored, meaning that it cannot "effectively [suppress] a large amount of speech that adults have a constitutional right to receive and to address to one another . . . if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[161] The Court explains that, "[i]n considering this question, a court assumes that certain protected speech may be regulated, and then asks what is the least restrictive alternative that can be used to achieve that goal."[162] The Court employs this test "to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to ensure that legitimate speech is not chilled or punished."[163]

A number of factors are relevant to a determination of whether a statute is narrowly tailored.[164] A review of prior Supreme Court cases

159. *Id.* at 205, 207 (quoting S. Rep. No. 106-141, at 7 (1999)).

160. *See Ashcroft III*, 542 U.S. 656, 665 (2004) (quoting *Reno I*, 521 U.S. 844, 874 (1997)).

161. *Id.*

162. *Id.* at 666.

163. *Id.*

164. While some restrictions on speech survive First Amendment scrutiny primarily

suggests that statutes with the following characteristics are more likely to survive strict scrutiny: (1) statutes that are not "prior restraints" in that they do not prevent speech; (2) statutes that allow individuals to opt-in to the protections rather than imposing them on everyone; (3) statutes that impose minimum burdens; (4) statutes that cannot be replaced with a less restrictive but effective alternative; (5) statutes that provide sufficient procedural protections and are not overly vague or broad. The following subsections explore ICPA's likely inclusion of these factors, mitigating in favor of its constitutionality.

1. No prior restraint

The Supreme Court has declared that "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights."[165] By definition, prior restraints give "public officials the power to deny use of a forum in advance of actual expression."[166] Indeed, prevention of such prior restraints is the primary purpose of the First Amendment.[167]

ICPA creates no regime of censorship and gives the government no right of prior review or screening of speech. Its enforcement depends on individual consumer identification and complaint following publication of speech, and then upon administrative and court authority. Under ICPA, an administrative agency[168] that receives a complaint may only request removal of violating speech if a Web publisher Posts Obscene or Child Pornography content on an Open Port or if a Content Publisher Posts content Harmful to Minors on a Community Port.[169] The speaker who knowingly and

because they target purely commercial speech or are justified as a regulation of secondary effects, these elements are not essential to justifying regulation. The Supreme Court upheld the Pandering Mail Act based on the countervailing consideration of "the right of every person to be 'let alone'" as opposed to the fact that the Act arguably targeted commercial speech. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 736 (1970).

165. Tory v. Cochran, 544 U.S. 734, 738 (2005) ("[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights." (citing Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976))).

166. Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 553 (1975).

167. *See id.*

168. ICPA is currently drafted naming the FCC in this role, but another possible agency is the National Telecommunications and Information Administration (NTIA) in the Federal Trade Commission. *See* Preston, *supra* note 57, at 1476.

169. *See id.* at 1471 app. § II(1).

intentionally Posts the violating speech may be subject to penalties or damages following court direction.[170] In the case of material that is Harmful to Minors—that is, constitutionally protected speech—the speaker has a fully viable alternative: to post the same material on an Open Port.[171]

2. Opt-in consumer choice

Under ICPA, individual Service Consumers may choose to continue to receive all Internet Ports as in the past.[172] Alternatively, individual consumers may choose to receive only the Internet content found on the Community Ports.[173] In both *Rowan* and *Mainstream Marketing Services, Inc.*, the courts recognized that opt-in regulations decrease government involvement, while still allowing individuals the choice to "erect a wall" that no one can "penetrate without . . . acquiescence."[174]

In *Mainstream Marketing*, the Tenth Circuit stated that the Do-Not-Call Registry Act was narrowly tailored to serve the government's interest because "its opt-in character ensures that it does not inhibit any speech directed at the home of a willing listener."[175] The idea that an opt-in regulation is less restrictive than a direct prohibition of speech applies not only to traditional door-to-door solicitation but also to regulations seeking to protect the privacy of the home from unwanted intrusions via telephone, television, or the Internet.[176]

ICPA's objective, as is the objective of the Pandering Mail Act (which was upheld in *Rowan*), is simply to "protect minors and the privacy of homes from [sexually explicit] material[s] and to place the judgment of what constitutes an offensive invasion . . . in the hands of the addressee."[177] And, unlike previous attempts to regulate Internet pornography, which sought to criminalize the transmission on all Internet ports of all pornography, including speech that is

170. *See id.* § III(8)(1).

171. *See id.* at 1476–77.

172. *See generally id.*

173. *See generally id.*

174. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970).

175. Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228, 1238 (10th Cir. 2004), *cert. denied*, 543 U.S. 812 (2004).

176. *See id.* at 1242.

177. *Rowan*, 397 U.S. at 732.

legal for adults, ICPA seeks only to achieve the government's goal "of maximiz[ing] user control over what information is received by individuals, families, and schools who use the Internet."[178]

3. ICPA imposes a minimal burden on speech

ICPA requires Web publishers of content that is Harmful to Minors[179] to configure their Server to broadcast their content via Open Ports.[180] The content is not altered in any way, the configuration is not visible to those who access the content, and all Internet users who have not affirmatively requested their ISP to limit their service to Community Ports may continue to access that content with no change in method or effort.[181] ICPA does not include any bans on speech and does not prevent any willing adults from speaking or hearing protected speech (such as pornography).[182]

Channeling technology currently exists, is free, and requires only minimal effort in configuring a Server, much like designating pick up by UPS or by Federal Express. The configuration code for adult content is free;[183] the burden in time and effort is negligible[184] and may legitimately be placed on the speaker who chooses to make low-value speech.[185]

Because of this, the burdens on speech imposed by ICPA are minimal. Both the Supreme Court in *Rowan* and the Tenth Circuit in *Mainstream Marketing* recognized that property owners should not carry the burden of preventing the delivery of unwanted speech—if someone is burdened with the responsibility of directing speech only to willing listeners, it should be the sender.[186]

178. 47 U.S.C. § 230(b)(3) (1998).

179. For the ICPA definition of this term, see *supra* note 98.

180. *See generally* Preston, *supra* note 57.

181. *See generally id*.

182. See *id*. at 1489–90 for a discussion of the chilling effect on legitimate fringe speech posted by independent bloggers, etc.

183. *See supra* Part III.B.

184. *Id*.

185. *See* Young v. Am. Mini Theatres, Inc., 427 U.S. 50, 61 (1976) ("[T]here is surely a less vital interest in the uninhibited exhibition of material that is on the borderline between pornography and artistic expression than in the free dissemination of ideas of social and political significance."); *see also* R.A.V. v. City of St. Paul, 505 U.S. 377, 432 (1992).

186. *See* Sable Commc'ns, Inc. v. FCC, 492 U.S. 115 (1989). In *Sable*, the Court ruled that a company that purveys material that is of low constitutional value (i.e., obscene in some of the service areas while only indecent in others) rightly can be made to "bear[ ] the burden of

The court in *Mainstream Marketing* also noted that the new technology that allows people to program their phones in an attempt to detect or block telemarketers is the same technology that is allowing telemarketers to circumvent these efforts.[187] The parallel to Internet filters and other recipient-driven screening devices is obvious. Americans who wish to avoid certain kinds of speech invading their private property should not have the burden of purchasing, installing, maintaining, and relying on filters, even if the filters are effective and available at any cost.

Similarly, rather than require individuals to demonstrate a legitimate interest in refusing to accept each particular item of mail under the Pandering Mail Act, the Supreme Court in *Rowan* ruled that a speech regulation can be broad enough to cover speech that may be perfectly harmless.[188] The Act, discussed in *Rowan*, prohibits the sender from mailing any material to an addressee after the addressee asks to have his or her name removed from the sender's mailing list, even if subsequent mailings are harmless.[189] The Court reasoned that "the citizen cannot be put to the burden of determining on repeated occasions whether the offending mailer has altered its material so as to make it acceptable. Nor should the householder have to risk that offensive material come into the hands of his children before it can be stopped."[190]

Take particular note of this last sentence. The Court, familiar with the world of accessible mailboxes on porches and streets, recognizes that children may easily stumble upon materials put into such boxes before the parent can intervene. The same is certainly true of the Internet. By conceptualizing one's computer as a repository of messages easily available to anyone in the house, the argument that a parent should be able to restrict outsiders' access to that repository becomes particularly persuasive.

The extent to which children today can access Web materials that their parents may never find suggests that the reasons for restricting placement in a family's computer repository are vastly more

complying with the prohibition on obscen[ity]." *Id.* at 126.

187. *See* Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228, 1245 (10th Cir. 2004), *cert. denied*, 543 U.S. 812 (2004).

188. *See* Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 730, 740 (1970).

189. *See id.*

190. *Id.* at 738.

compelling than the reasons for restricting access to a family's mailbox. Parents lack effective tools to intervene and remove the material on the computer before a child intercepts it, and parents may never even know which messages their children are retrieving from the Internet. Thus, it is far more effective to sort content at the originating server than to attempt to sort it at the receiving end. The ICPA option is also more supportive of the constitutionally protected right of parental choice.

4. No reasonable less restrictive alternatives

Despite their recent approval in *Gonzales*, filters cannot serve as a less restrictive alternative to ICPA. Filters fail to adequately protect children for several reasons. First, filters underblock, failing to exclude a startling amount of pornography. Second, filters overblock, needlessly excluding useful content. Third, filters are expensive and intimidate parents. Fourth, filter companies may intentionally block harmless information. Finally, filters are easily circumvented by technologically-savvy children. Because of such shortcomings, filters are not an effective alternative.

First, filters inevitably underblock.[191] Well-funded pornographers continue to develop new techniques, such as spelling deviations and "imaged" wording, to bypass even the best filters.[192] The *Gonzales* court was satisfied with filters that are ninety-five percent effective. And while the court found such effectiveness comforting, most parents would be appalled to learn that, despite an expensive, commercial-grade, updated, and properly installed and maintained filter, up to thirty-five million pages of sexually explicit material remain unblocked on their home computer.[193]

191. *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 795–97 (E.D. Pa. 2007).

192. Jared Chrislip, *Filtering the Internet like a Smokestack: How the Children's Internet Protection Act Suggests a New Internet Regulation Theory*, 5 J. HIGH TECH. L. 261, 272 (2005) ("Web site publishers can . . . use image files to place words on the screen that a filter cannot 'see.'"); *see also* Jacob A. Sosnay, *supra* note 54, at 480 (explaining that "savvy Internet pornographers [are] using creative techniques to get around the filtering software's criteria").

193. In *Gonzales*, Judge Reed accepted expert Zook's testimony that the Internet contains between 275 million to 700 million pages of sexually explicit material. *Gonzales*, 478 F. Supp. 2d at 788. Even if filters can be assumed reliable to ninety-five percent, the remaining five percent of the 700 million pornographic pages on the Internet still equates to 35 million unblocked pages of pornography available for child consumption.

Second, filters overblock.[194] As parents increase the restrictive levels of their filters, the software inevitably blocks more and more innocuous material. "Filters generally cannot construe the context of the supposed objectionable term or phrase" and will therefore "deny access to innocuous web pages."[195] An obvious example is a filter that uses textual analysis set to block pornographic Web sites using the word "breast." It would also deny access to Web pages with information on women and cancer ("breast" cancer), neonatal health ("breast" feeding), and chicken recipes (chicken "breast").[196] Similarly, a block on the word "sex" blocks sites that have data on gender studies, dog breeding, and color blindness. Many filters needlessly block useful information such as medical sites, content dealing with homosexuality, safe sex material, and even educational material on the harms of pornography.[197]

Third, filters fail to protect a child if parents neglect to use a filter or if an unsecured, unfiltered wireless Internet connection enters the home from a neighboring house or business.[198] Indeed, filter use in the United States is not uniform; nearly fifty percent of children live in homes where filters are not employed.[199] Many parents are intimidated by the time, cost, and technical know-how associated with choosing among, purchasing, and installing a filter. And, many parents must then rely on the resident teenager to install and maintain the filter.

Fourth, filter companies may intentionally censor harmless information. Such a threat is described by Lawrence Lessig, a prominent scholar in free speech jurisprudence:

> There is a lot of good evidence about how poorly this technology filters cyberspace: how it filters the wrong type of material. There are also more insidious examples of what the companies that release

194. *See id.* at 797; Chrislip, *supra* note 192, at 271.

195. Chrislip, *supra* note 192, at 271.

196. *See id.*

197. *See* Christopher D. Hunter, *Internet Filter Effectiveness—Testing Over- and Under-Inclusive Blocking Decisions of Four Popular Web Filters*, 18 SOC. SCI. COMP. REV. 214, 221 (2000).

198. *See* Cheryl B. Preston, *WiFi in Utah: Legal and Social Issues*, UTAH B.J., Sept.–Oct. 2007, at 29.

199. *See* AMANDA LENHART, PEW INTERNET & AM. LIFE PROJECT, PROTECTING TEENS ONLINE, at i (2005), *available at* http://www.pewinternet.org/pdfs/PIP_Filters_Report.pdf (explaining that only a little over "half (54 %) of internet-connected families with teens now use filters").

> this software do. For example, if you become known as a critic of that software, mysteriously your Web site may appear on the list of blocked Web sites, which becomes an extraordinary blacklist of banned books. The problem with this blacklist of banned books is that the public cannot look at it.[200]

Private filtering companies refuse to provide lists of sites they block and why. Lessig maintains that government regulation is more effective and more appropriate than filters because the government may be held accountable.

> If you disagree with something Net Nanny blocks what can you do about it? The answer is nothing. You could complain to the company that produces Net Nanny but if they disagree with your complaint, too bad so sad. But if you disagree with a block that's imposed by the law, then that . . . block can be challenged in a court because any law, as it restricts speech, must be justifiable against the standards of the first amendment. So, unlike private blocks, which are imposed and difficult to discern, these public blocks, even though they're hard to figure out, would still be challengeable and testable according to the standards of the first amendment.[201]

Given the core First Amendment value—a citizen's right to access the information he or she wants to hear—it cannot be a superior approach to give control over Internet content to a private party subject to no oversight or standards and with an unknowable agenda. It is one thing for a speaker to choose not to speak on a Community Port, as it is for a speaker to choose not to speak at all; but it is quite another to delegate to an intermediary commercial

200. Lawrence Lessig, *Constitutional Law and the Law of Cyberspace*, *in* NATIONAL RESEARCH COUNCIL (U.S.), COMMITTEE TO STUDY TOOLS AND STRATEGIES FOR PROTECTING KIDS FROM PORNOGRAPHY AND THEIR APPLICABILITY TO OTHER INAPPROPRIATE INTERNET CONTENT STAFF(CB), TECHNICAL, BUSINESS, AND LEGAL DIMENSIONS OF PROTECTING CHILDREN FROM PORNOGRAPHY ON THE INTERNET: PROCEEDINGS OF A WORKSHOP 110, 112 (2002), *available at* http://newton.nap.edu/html/protecting_children/ch17.html.

201. Lawrence Lessig, Video: A Modest Proposal for Zoning Immodesty (Mar. 22, 2007), *available at* http://www.lessig.org/blog/archives/003738.shtml. Professor Lessig first presented this proposal to Congress; he then released it to the public in video form on his blog. The video may be accessed by clicking the "play" button on the Google video player, which is posted on the above-described blog page. For those who would like to download the video, Professor Lessig has also provided a link on the page. The quoted section begins about thirteen minutes into the video.

entity the power to block speech without any obligation to disclose its reasons or criteria.

Finally, even children in protected environments can easily circumvent filters. While filters may be better than nothing and may help prevent most inadvertent forays into Internet pornography, they are little more than a speed bump in the way of those who seek pornography sites. "[T]he high level of computer literacy of children allows them to bypass filters through tricks that go undetected by their less computer savvy parents."[202] The National Research Council identified various ways in which children can get around filtering software.[203] For example, youth can uninstall the filter, disable the filter (in many homes, the "resident teenager serves as the de facto system administrator because of superior technical knowledge"), access the Web page indirectly through a proxy, find a different click route to the page, and "manipulate the reload/refresh and back/forward keys."[204]

Judge Reed in *Gonzales* concluded: "It is difficult for children to circumvent filters because of the technical ability and expertise necessary to do so by disabling the product on the actual computer or by accessing the Web through a proxy or intermediary computer and successfully avoiding a filter on the minor's computer."[205] This may perhaps be true for very young children, but a child in junior high who has had any computer training or who has friends with such training is likely to be more than sufficiently technologically capable. In fact, a simple Google search of the word "proxy" (which almost any child can perform) returns multiple links to Web pages that explain how to use a proxy to bypass a filter to get to pornography.[206] There are advertisements for proxy sites on pages children access and in "spam" e-mails. The teenagers interviewed by CP80 and Living Biography stated that they had never waited for

202. Steven E. Merlis, *Preserving Internet Expression While Protecting Our Children: Solutions Following* Ashcroft v. ACLU, 4 NW. J. TECH. & INTELL. PROP. 117, 128 (2005).

203. *See* DICK THORNBURG, NATIONAL RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET § 12.1.2, at 281 (2002).

204. *Id.*

205. ACLU v. Gonzales, 478 F. Supp. 2d 775, 795 (E.D. Pa. 2007) (finding 108) (citations omitted).

206. ICPA's definition of "Content Publisher" includes any person who "uses an IP address to . . . Proxy, a Communication." *See* Preston, *supra* note 57, at 1471 app. § V(12). Thus, a person who facilitated the circumvention of a filter to obtain pornography could be held liable under ICPA.

more than a few minutes for a reply on the AOL or MSN discussion blog telling them how to access a pornography site through a proxy or around the filter.[207] Thus, the only feasible way to stop a computer user from accessing Internet pornography is to prevent such materials from coming into the computer in the first place.[208] A filter may prevent someone from accidentally stumbling into lurid pornography sites, but it will not stop someone who is looking for it.

ICPA solves many of the problems associated with filters. In fact, the very reasons the courts provide for finding filters less restrictive and more effective than COPA, support the argument that ICPA is a more reasonable alternative. For example, in *Ashcroft III*, the plurality opinion of the Supreme Court suggested that blocking and filtering software is an "alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[209] The Court considered filters to be *less restrictive* because "they impose selective restrictions on speech at the receiving end, not universal restrictions at the source."[210] ICPA also imposes restrictions by choices at the receiving end. The *Ashcroft III* Court considered filters more *effective* as a means to achieve the government's goal because filters could block pornography posted on the Internet both in the United States and in foreign countries.[211] The problem of foreign pornography is overstated and the Ports Concept provides a scheme that permits more efficient blocking of foreign content.[212] Also, the

207. Film clips on file with author.

208. ICPA is fundamentally different than the legislation found to be unconstitutional in *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803 (2000). That legislation was found to be unconstitutional under a strict scrutiny analysis not because it was deemed to be too restrictive, but because the Government had failed to demonstrate that there was a nation-wide problem in need of as drastic a solution as a ban on speech. *Id.* at 823. Also, the Government failed to prove that a well-publicized alternative to mandatory signal bleed-blocking, which would be less restrictive, would not be effective. *Id.* There is also ample evidence that unwanted Internet Communications that are Obscene, Child Pornography, or Harmful to Minors enter homes all over the United States. So, where the statute at issue in *Playboy* lacked proof of its relative restrictiveness, as well as an identifiable problem to solve, ICPA has both.

209. *Ashcroft III*, 542 U.S. 656, 666–67 (2004).

210. *Id.* at 667. Also, receiving end restrictions do not "condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished." *Id.*

211. *See id.*

212. *See* Cheryl B. Preston, *Offshore Porn Is a Flimsy Excuse* (forthcoming 2008) (copy on file with the author).

Court argued that filters could be applied to "all forms of Internet communication, including e-mail, [and] not just communications available via the World Wide Web."[213] Again, ICPA covers all forms of Internet Communication.

With similar logic, the district court on remand in *Gonzales* agreed that filters were a less restrictive and more effective alternative to COPA.[214] The court concluded that filters are less restrictive than COPA's provisions for three reasons: (1) filters "impose selective restrictions on speech at the receiving end, not universal restrictions at the source;" (2) filters preserve anonymity since adults, with or without children, "may gain access to speech they have a right to see without having to identify themselves or provide their credit card information;" and (3) filters cause little or no speech chilling because "promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."[215] Judge Reed also faulted COPA for applying only to the "surface web," or transfers that occur over the "HTTP or a successor protocol,"[216] and for failing to protect minors from a significant amount of Internet pornography originating outside the United States.[217]

ICPA is less restrictive than COPA precisely because it allows "selective restrictions on speech at the receiving end,"[218] preserves anonymity, and does not condemn speech as criminal. The remedies in ICPA are primarily administrative and civil. Criminal sanctions are only available for failing to honor a court order.[219] ICPA simply allows those users who do not want to access adult content to select an Internet service without it. Even though speech is categorized under ICPA, the effective and legal dissemination of such speech is not curtailed. Those who desire to gain "access to speech they have a right to see"[220] need do nothing. They simply continue to receive an Internet service that includes both Community and Open Ports.

213. *Ashcroft III*, 542 U.S. at 668.
214. *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 810–11, 813–16 (E.D. Pa. 2007).
215. *Id*. at 813–14 (quoting *Ashcroft III*, 542 U.S. at 667).
216. *Id*. at 788, 798.
217. *See id*. at 810.
218. *Id*. at 813 (quoting *Ashcroft III*, 542 U.S. at 667).
219. *See* Preston, *supra* note 57, at 1471 app. § III(9).
220. *Id*.

In addition to being less restrictive on speech, ICPA also provides a much more effective solution to protecting children from the harms of Internet pornography than does COPA. COPA's language addresses only material on port 80, and thus it does not provide any solution for material sent over port 25, or e-mail. ICPA contemplates ranges of ports designated as "Community," and ranges designated as "Open." Within the range of Community Ports would be all of the variety of port uses now available, including port 25, for e-mail. The Open Port range would include a parallel set of ports for such purposes so that all Internet-transmitted content could be as easily sent in either range. Thus, within the Community Port range, regardless of whether Internet users post prohibited content to the Internet through port 80 (Web browsing), port 21 (file transfers), or port 25 (e-mailing) they will be in violation of ICPA.

In sum, filters are not a less restrictive nor equally effective alternative to ICPA because of the failings of filters and the more appropriate scope of ICPA. When applied to ICPA, the past judicial reasons for preferring filters over COPA point to ICPA as a more effective solution.

5. Not under-inclusive

ICPA is also more appropriate than previous attempts at regulation because it is not under-inclusive. First, it covers e-mail and other Internet uses, not just the World Wide Web or port 80.

Second, it covers noncommercial pornographers, although the penalties are graded to account for the economic resources of commercial Web publishers. Congress's stated objective for the CDA and COPA was to protect children from age-inappropriate, sexual material on the Internet. It makes no sense to regulate only commercial pornographers while permitting individuals with motives perhaps more sinister than money to develop multitudes of Web sites with sexually explicit content aimed at attracting children. Moreover, amateur sites such as YouPorn, Pornotube, and Megarotic are becoming even more popular than paid pornography sites.[221] The

221. *See* Claire Hoffman, *Obscene Losses*, CONDÉ NAST PORTFOLIO.COM, Nov. 2007, http://www.portfolio.com/culture-lifestyle/culture-inc/arts/2007/10/15/YouPorn-Vivid-Entertainment-Profile. YouPorn is the No. 1 adult site in the world; Vivid.com, a pay site, is ranked 5061. *Id.*

burden is so minimal and the procedures for administrative resolution so generous, that ICPA much better focuses on the harm identified by Congress.

Third, ICPA is crafted to provide an architectural and legal regulatory scheme that will be effective in addressing the majority of the pornography posted on the Internet. ICPA regulates pornography originating in the United States, and most pornography available on the Internet is posted from locations subject to U.S. jurisdiction. ICPA also provides a framework to allow parents to block inappropriate foreign sites.

Therefore, ICPA is not under-inclusive because, unlike COPA, ICPA regulates all Internet uses, all pornographers, and a vast majority of the harmful material now available to American children.

6. Procedural protections

In *Rowan*, the Court determined that the Pandering Mail Act satisfies the constitutional requirement of the "opportunity to be heard upon such notice and proceedings as are adequate to safeguard the right for which the constitutional protection is invoked," even though the first level of enforcement was administrative.[222] The Pandering Mail Act requires the Postmaster General to notify the sender of sexual material of the addressee's request to stop such mail, allows the sender fifteen days to respond to the Postmaster's notice of violation, provides the sender with an opportunity to have an administrative hearing to determine if it violated the Pandering Mail Act, and provides a second hearing for the Attorney General to enter a compliance order.[223] Even though the Postmaster General's prohibitory order may come without an administrative hearing, the Supreme Court in *Rowan* ruled that the Pandering Mail Act did not violate due process because it did not impose immediate sanctions on the sender who did not comply with that order; it only led to further proceedings.[224]

The same is true of ICPA. If a Content Publisher receives a compliance order from an administrative agency that it believes was improperly issued or ungrounded, the Content Publisher may

222. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 738 (1970) (quoting Anderson Nat'l Bank v. Luckett, 321 U.S. 233, 246 (1944)).

223. *See id.* at 738–39.

224. *See id.* at 739.

request an administrative hearing with that agency.[225] ICPA also provides for a further hearing in a federal district court, if requested.[226] These precautions, plus the requirement that any complaint concerning a possible violation be submitted under penalty of perjury,[227] protect against specious complaints.

While it is true that, under Supreme Court precedents, any attempt to define material that is "Obscene" or "Harmful to Minors" must allow for court interpretation in individual circumstances, the lack of a mechanical, precise definition is not fatal on vagueness grounds. The Supreme Court has already ruled that use of the *Miller* test as a basis for such definitions is constitutional.[228]

Moreover, the Supreme Court in *Rowan* concluded that the Pandering Mail Act is not fatally vague because senders of speech are not open to "risk or detriment without . . . fair warning of the nature of the proscribed conduct."[229] Senders know precisely what to do when they receive a compliance order, and senders are only exposed to criminal sanctions if they continue "to mail to a particular addressee after administrative and judicial proceedings."[230] Similarly, the ICPA definitions provide fair warning of the proscribed conduct.[231] ICPA precisely defines what a Content Publisher is required to do once it receives Notification of a potential violation.[232] Also, under ICPA, Content Publishers are only exposed to criminal sanctions if they refuse to remove content from the Internet once there has been a Final Determination[233] that the Communication violates ICPA.[234]

C. Response to Potential ICPA Roadblocks

As part of the Kids Online! conference, Professor Dawn Nunziato suggested several potential roadblocks to the effective

225. *See* Preston, *supra* note 57, at 1471 app. § III(3)(v).
226. *Id.* § III(8).
227. *See id.* § III(2)(iii)(e).
228. *See Ashcroft I*, 535 U.S. 564, 585–86 (2002).
229. *Rowan*, 397 U.S. at 740.
230. *Id.*
231. *See* Preston, *supra* note 57, at 1471 app. § II.
232. *See id.* § III.
233. This only comes after an appeals process. *See id.*
234. *See id.*

implementation of ICPA. This section responds to each of these roadblocks.

1. Web publishers will choose to serve on Community Ports

Professor Nunziato needlessly worries that Web publishers will choose not to post to the Community Ports for fear that something on their pages may be challenged under ICPA.[235] Those with highly questionable content may do so, but the market demands created by an ICPA-supported system will motivate non-adult publishers to establish a presence on Community Ports. The marketing potential for ISPs who offer family friendly packaging will be enormous.

Realistically, who is likely to subscribe to Community Port-only Internet service? We can safely assume that at least half of the people who are now purchasing filters for their computers will prefer an option that is much cheaper, easier, and less demanding on the speed and capacity of a computer system.[236] Surely, more than half of the nineteen million homes where filters are currently used to protect teens would be likely to purchase a Community Port-only service.[237] Add to this every user that currently has an AOL account and has requested the most restrictive level of filtering.[238] Then add a percentage of those who have asked for a less restrictive AOL filter or a filter block provided by any other ISP.[239] Add to this number of

235. *See* Nunziato, *supra* note 4, at 1578 ("Because ICPA imposes optional and technologically straightforward requirements, the burdens it imposes on content providers are minimal, but so are the likely benefits accruing from the statute.").

236. According to a study conducted by Pew, "54% of internet-connected families with teens now use filters." LENHART, *supra* note 199, at i.

237. Pew Internet & American Life Project, Reports: Family, Friends & Community (March 17, 2005), http://www.pewinternet.org/PPF/r/152/report_display.asp ("In all, about 19 million youth live in homes with internet connections and the number of children living in homes with filters has grown . . . to 12 million today.").

238. ACLU v. Gonzales, 478 F. Supp. 2d 775, 791 (E.D. Pa. 2007) ("AOL's filtering product enables parents to choose from four different age settings: general (unrestricted); mature teen; young teen; and kids only.").

239. All of the major ISPs offer a "filtered" connection choice, although it is unclear how effective these are since no ISPs will disclose any data or even a list of blocked sites or blocking criteria. *See, e.g.*, AT&T WorldNet Service Offers Free Cyber Patrol Software for a Year, http://worldnet.att.net/general-info/kidsafe.html; Earthlink Offers Free Parental Controls, http://www.earthlink.net/software/free/parentalcontrols/; MSN Offers Free Parental Controls, http://join.msn.com/dialup/features; Verizon Gives Free MSN Software (which includes parental controls), http://www.verizon.net/micro/betterway/faq.asp (last visited Nov. 20, 2007). For an extensive list of other ISPs who offer filtered service, see http://www.google.com/alpha/Top/Computers/Internet/Access_Providers/Filtered (last

likely consumers most elementary schools in the United States,[240] most middle schools,[241] all employers who have a "no porn at work" policy, and two-thirds of public libraries.[242]

Experience in a conservative religious community makes clear two things: (1) many of America's active religious adherents will opt for Community Ports, including most conservative Catholics, orthodox Jews, active members of the Church of Jesus Christ of Latter-day Saints, and members in other religious traditions where leaders have taken a firm stance in opposition to pornography or to children's access to pornography; and (2) the economic clout of members of such religious groups is considerable. In addition, we can fairly assume that some parents who do not have filters would choose a Community Port-only package if one were advertised or offered by ISPs, even if they have thus far failed to realize the extent of the Internet pornography problem or overcome the intimidation of the filter section at a computer store.

As becomes apparent, the number of consumers choosing Community Port-only plans will be more than enough to motivate Web publishers to have a presence on Community Ports, even if no one from the "non-filtering" geek population chooses to order Community Ports-only access.

a. Dot Kids is inapposite. Professor Nunziato compares Community Port access to Dot Kids (.kids.us), a largely unsuccessful attempt to carve out a separate space on the Web for children. The comparison is unpersuasive.

The Dot Kids Implementation and Efficiency Act of 2002 (Dot Kids Act) was signed into law on December 4, 2002.[243] This law

visited Nov. 20, 2007).

240. "The U.S. Department of Education estimates that 90 percent of K-12 schools today employ some sort of web filtering technology in adherence with guidelines set forth as part of the Children's Internet Protection Act . . . ." Corey Murray, *Study: Overzealous Filters Hinder Research*, ESCHOOL NEWS, Oct. 13, 2005, http://www.eschoolnews.com/news/top-news/index.cfm?i=36606&CFID=1203343&CFTOKEN=75739672.

241. "In a recent poll of 295 teachers, technology directors, school board members, and other educators attending the national Technology+Learning conference, 51 percent said they were currently using censorware for all or some students in their district." Electronic School Online, *Censorware: How Well Does Internet Filtering Software Protect Students?*, http://www.electronic-school.com/0198f1.html (last visited Nov. 20, 2007).

242. "Just under two-thirds (65%) of all libraries filter some Internet terminals, regardless of CIPA." Norman Oder, *Ripple Effects: Budgets Grow Modestly, but Energy Costs Cloud the Horizon*, LIBR. J., Jan. 15, 2006, at 59, 60.

provides for the creation of a second-level Internet domain under the ".us" country code, a ".kids" domain.[244] It restricts information on the site to material that is "suitable for minors" and "not harmful to minors."[245] The Dot Kids domain was never intended for children age thirteen and older.[246] The guidelines for Web sites given a Dot Kids domain name are found on the kids.us site.[247] The Dot Kids Act requires Web publishers wanting to post a Web site with the ".kids.us" domain name to certify that the content on the Web site is "suitable for minors" and not "harmful to minors."[248] There are no hyperlinks or chat rooms.[249] The Dot Kids guidelines require monitoring for "predatory behavior by adults, exploitation[,] or illegal actions," and all content must be both psychologically and intellectually appropriate for minors, defined as children under thirteen.[250] In addition, the Dot Kids Act required that Web sites comply with the Children's Online Privacy Protection Act.[251]

Parental awareness of Dot Kids is so low that even those who use the Internet regularly were unlikely to know of its existence. Web site owners argue that Internet users are so accustomed to .com that they will never take the effort to use Dot Kids.[252] In fact, at the time when Dot Kids was introduced, parental knowledge of the extent and nature of dangerous Internet content discoverable by kids was also much lower than it is now. Dot Kids was not marketed: it was not a choice offered by commercial ISPs; it was not an option mentioned in monthly service bills; it was not advertised, even by the government. An ISP that sees the marketing potential of offering a

243. Dot Kids Implementation and Efficiency Act of 2002, Pub. L. 107-317, 116 Stat. 2766 (2002) (codified at 47 U.S.C. § 941 (2002)).

244. *Id.* § 2(b)(1), 116 Stat. 2766.

245. 47 U.S.C. § 941(a) (2002).

246. *See* M. Megan, *Virtual Lollipops and Lost Puppies: How Far Can States Go To Protect Minors Through the Use of Internet Luring Laws*, 14 COMLCON 503, 508–09 n.33 (2006).

247. *See* Kids.us Content Policies, http://www.kids.us/content_policy/content.html (last visited Nov. 21, 2007).

248. 47 U.S.C. § 941(a) (2002); *see also Kids.us Content Policies, supra* note 248.

249. *See id.*

250. *Id.*

251. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2000); NEUSTAR, INC., KIDS.US CONTENT POLICY: GUIDELINES AND RESTRICTIONS 7 (2003), http://www.kids.us/content_policy/content_policy.pdf.

252. *See* Anick Jesdanun, *Not Everyone On Line with Kid-Safe Domain*, TULSA WORLD, May 12, 2002, at 10.

Community Ports-only option will do its best to be sure that its customer base is aware of that option's advantages.

Second, Web publishers have to "move" to post content on the Dot Kids domain, whereas under ICPA, port 80 (on which all HTTP content is now served) will be designated as a Community Port. Those who choose to Post material intended to appeal to the prurient interest of Minors, or material that as Sexually Explicit Conduct, will need to configure their Servers to Post that content on an Open Port. It is only fair that the purveyors of low-value speech bear the burden (although slight) of making a change rather than parents.

Third, those who wish to limit Internet use in their home to material appropriate for children bear the burden of typing in the ".kids.us." It is impossible to limit the computer's access to other domains. Thus, unless the parents are present to ensure the correct domain address was entered every time, Dot Kids provides no restrictions on a child's curiosity.

Fourth, the name of this domain itself limits the sense of its applicability. "Kids" suggests that the material there is intended for small children, a "playground" mentality.[253] Many assume the domain is for preschool-aged children and that it is only the province of Disney and Nickelodeon.[254] The name certainly does not suggest that this is the place for fifth graders to conduct research for state reports, look up words in the dictionary, or check on news about the new Spiderman movie. Certainly, most would not consult a "kids" domain to find information about teens' favorite music and movies.

Thus, because of the many ways that Dot Kids is not comparable to a Community Ports plan, the failure of Dot Kids to attract a broad base of users is not persuasive evidence of the market demand for Community Ports. And, because of the market segment likely to use Community Ports, it is unlikely that many businesses or information providers will refuse to have a presence there.

b. The National Zoo will publish on Community Ports. Professor Nunziato wrongly surmises that the National Zoo might forego

253. *See* Alice G. McAfee, *Creating Kid-Friendly Webspace: A Playground Model For Internet Regulation*, 82 TEX. L. REV. 201, 218–19 (2003).

254. *See* Kevin W. Saunders, *The Need for a Two (Or More) Tiered First Amendment To Provide for the Protection of Children*, 79 CHI.-KENT L. REV. 257, 259 (2004).

publishing on a Community Port for fear that depictions of animal sexuality might violate ICPA.[255] First, even if ICPA applied to zoo animals' sexual activity,[256] most zoo administrators will not choose to alienate existing and potential patrons who use Community Port-only plans. The biggest single constituent group for zoos are children and their parents, who pay for admission tickets, food and candy, extra exhibits, shows, fuzzy animals, T-shirts, jammies, and rental strollers. Refusing to have a Web site on Community "family friendly" Ports would be a poor business decision indeed. Moreover, the zoo could easily choose to be on a Community Port and then provide a seamless link to an Open Port to display images of Explicit Sexual Conduct among animals that fits within the definition of "Harmful to Minors."

However, if zoo administrators want to post images that "are designed to appeal to, or [are] designed to pander to, the prurient interest of Minors," and "depict Sexually Explicit Conduct," and, in addition, "lack serious . . . scientific value for Minors,"[257] then most families will be grateful that such images are not available on their home computers. Zoos are largely supported by public funds. City, county, and state officials would have a hard time explaining why the zoo refuses to place its Web site on a Community Port. Give voters ICPA's definition of Harmful to Minors, and it is unlikely they will support the zoo's efforts to serve such material on the Web, even if, in fact, any conduct between natural animals could ever be said to be designed to appeal to a prurient interest or to be without scientific

255. *See* Nunziato, *supra* note 4, at 1580.

> Given that the Zoo's Web site may contain content that, for example, depicts or describes animals' sexual activity (and given that such conduct could fall within the statutory definition of Harmful to Minors content), the publisher of the Zoo's Web site might reasonably determine that the added benefit of publishing via a Community Port was not worth the risk.

Id. (citations omitted).

256. The ICPA definition of "Harmful to Minors" was originally written to include the reference to "Sexually Explicit Conduct" in the first clause, rather than the second. In this format, the modifiers of the first clause did not apply, i.e. designed to appeal or pander to a prurient interest. However, the modifiers of clauses two and three still moderated its application. As now written, the "Harmful to Minors" definition even more clearly excludes the kind of material Professor Nunziato uses as the example for the National Zoo illustration. *See supra* note 98.

257. For ICPA's definition of "Harmful to Minors," see *supra* note 98.

value. In short, most zoos have no interest in posting depictions that qualify under ICPA's definition as Harmful to Minors.[258]

2. The ICPA "stigma" is not unduly burdensome

Contrary to Professor Nunziato's assertion, ICPA's requirements do not impose a burden that "substantially and unconstitutionally restrict[s] speech."[259] Professor Nunziato acknowledges that designating Web pages for Open Ports is not technically burdensome, but she suggests that the designation would create an unconstitutional stigma.[260]

The code necessary to serve Web pages via Open Ports is invisible to Internet users; thus, Open Port subscribers may freely view pornography alongside Sesame Street with no perceptible label, restriction, or ranking attaching to the pornography.[261] Moreover, decades of precedent by the Supreme Court make it clear that, while adults may have a right to a reasonable alternative access to adult material, purveyors of adult material need not be given the key to the city.[262]

The burden on those who serve sexually explicit content is so slight, on the one hand,[263] and the government's interests of protecting minors, giving parents control of sexual education, and keeping unwanted speech out of private property[264] are so compelling on the other hand, that there is little room for arguing that those who disseminate depictions of sexually explicit conduct

258. *See id.*

259. *See* Nunziato, *supra* note 4, at ? {pinpoint} ("Although . . . the designation itself is not technologically burdensome, such a requirement would substantially and unconstitutionally restrict speech.").

260. *See id.*

261. Moreover, if the National Zoo, as Nunziato claims above, will be willing to move all zoo material to the Open Ports "just to be safe," there must not be much stigma. An entity depending on public largesse and the patronage of families with children would certainly be as sensitive to any "stigma" as anyone.

262. The opposite is the case; the Court has approved zoning restrictions on adult businesses. *See* Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986) (upholding city zoning ordinance prohibiting adult theatres from locating within 1000 feet from specified places, including homes and schools); Young v. Am. Mini Theatres, Inc., 427 U.S. 50, 71 (1976) (plurality opinion) ("[The] city must be allowed a reasonable opportunity to experiment with solutions to admittedly serious problems.").

263. *See supra* Part IV.B.3 (discussing the slight burden imposed by ICPA).

264. *See supra* Part IV.A (discussing the three compelling governmental interests served by ICPA).

that is without educational value for minors should not face any stigma from parents.

The Supreme Court has upheld zoning restrictions on adult businesses and even justified the presumption that crime and property destruction is a likely by-product of adult businesses.[265] Surely, the zoning of the Internet is no more stigmatizing. Furthermore, if a pornographer is allowed to argue that its work is stigmatized by Internet zoning, such pornographer's work is already stigmatized because, under *ACLU v. Gonzales*, we encourage, families, public libraries accepting federal funds, and schools to use filters that are intended for the precise purpose of blocking such material.[266] The use of filters for this very purpose has been positively supported by the Supreme Court.[267] Besides, this argument is inconsistent with the fear that venerable public institutions, such as the National Zoo, would choose to have Web sites on Open Ports rather than Community Ports. The stigma must not be that great.

3. ICPA does not overblock protected speech

a. The Constitution protects "unwilling listeners."[268] Professor Nunziato's claim that ICPA unconstitutionally overblocks protected speech[269] ignores a critical point: Community Port subscribers *choose* to block certain speech from their computers. Every American has the right to choose against receiving sexually provocative mailings or inviting protestors to have a rally on his or her property.[270] The

265. *See Renton*, 475 U.S. at 41; *see also* John Fee, *Obscenity and the World Wide Web*, 2007 BYU L. REV. 1691.

266. *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 814–16 (E.D. Penn. 2007) (finding that filters offer alternative protection for parents and their children).

267. United States v. Am. Library Ass'n, 539 U.S. 194, 207–08 (2003) (finding that a library's use of a filter constituted a collections decision, not an improper infringement on free speech).

268. Frisby v. Schultz, 487 U.S. 474, 485 (1988).

269. *See* Nunziato, *supra* note 4, at 1582.

> Accordingly, although ICPA imposes minor technological and financial burdens on content providers in designating which types of ports to publish their content over, it would likely operate to substantially restrict the speech available to those who receive content over Community Ports, and a reviewing court would likely find that it operated to substantially overblock harmful speech.

Id.

270. *See supra* Part IV.A.3 (discussing Supreme Court decisions protecting the privacy of property owners from intrusions such as sexually provocative mail and protestors).

ICPA scheme is purely "opt in."[271] Thus, if a computer owner affirmatively chooses to purchase a Community Port-only Internet access plan, no court would interpret the Constitution as requiring him or her to receive a broader range of speech.

Moreover, ICPA is unlikely to "overblock" to the extent that filters do.[272] Filter overblocking is caused by the difficulty programmers have in getting filters to "read" accurately the content on a Web page. No similar programming difficulty exists under a Ports Concept. The choice of what is appropriate on Community Ports and what is not is made by those who create and serve the content. They are certainly in the best position to know its nature. Reviewing courts should not insist on a system that requires employees at filter companies to view pornographic filth to determine what content to block. The protective approach that is least burdensome on Americans is one that puts the onus on those who choose to be exposed to and deal in sexually explicit material.

If Web publishers elect to limit the reach of their message and cause "overblocking" by not serving acceptable content on Community Ports, that is their choice. And if a consumer subsequently chooses the restrictions of the Community Ports, no court will claim that his or her decision is unconstitutional.

b. Adults may choose to limit impulse access. In another argument related to overblocking, Professor Nunziato complains that, unlike filters, Community Ports cannot easily be turned off and on to allow access to adult material.[273] As was stressed above, this complaint is misplaced, since the Internet user affected under the Ports Concept is the one who chooses the more restrictive Community Ports access, including the inability to turn it off on an impulse. Many who understand the risks of pornography will find most appealing the fact that the port restriction cannot be hacked, circumvented or changed

271. *See supra* Part IV.B.2.

272. Judge Reed considered expert testimony asserting that some filters overblocked up to 32.8% of benign Internet content but rejected that figure in favor of an alternate report setting the general overblocking rate at up to 11.03%. *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 795–96 (E.D. Pa. 2007).

273. *See* Nunziato, *supra* note 4, at 1582 ("In contrast, as contemplated under ICPA, the decision to receive communication only through Community Ports cannot be readily modified.").

without the adult Internet service purchaser going through the steps to call the ISP during business hours and verify identity.

Of course, the case of a library purchasing an Internet service is different than that of an individual choosing a service for a private computer. In *American Library Ass'n*, the Court appropriately emphasized that adults in such libraries may request a quick and easy filter disabling mechanism because the library, not its patrons, purchased the speech restricting filter—with a federal subsidy—and offered Internet service to members of the public who may have no other option for accessing the Web.[274] Under ICPA, a library may choose to have select computers with Open Ports access and such a filter to accommodate adult patrons.

No corresponding constitutional right inures to adults to use unfiltered Internet access in a private house. Parents have no obligation to provide guests, relatives, or adult children access to Internet pornography in their home, on their computer, and through an Internet access service they pay for. Homeowners who purchase an Internet access plan can agree on any limitations they like without implicating constitutional rights, except their rights to control their own private property and the education of their children and to prevent unwanted speech invasions.

Certainly, following the adoption of ICPA or another zoning regulation, some ISPs may decide to provide a service plan that makes only Community Ports available, except during certain hours of the day when Open Port access is included. And anyone who wants the option of quickly disabling a block may always subscribe to Open Ports and then install a filter that permits disabling. However, those who do not want computer users in their home to be able to turn off the filter compulsively at any time will, under ICPA, have a better choice.

4. Filters do not offer a less restrictive alternative to ICPA

Professor Nunziato, citing to Justice Kennedy's language in *Ashcroft III*, argues that the Court prefers regulations empowering end users rather than regulations limiting content providers. Thus, she argues that filters are a better alternative to ICPA.[275] However,

274. *See* United States v. Am. Library Ass'n, 539 U.S. 194, 209–12 (2003).

275. *See* Nunziato, *supra* note 4, at 1570 ("First, courts prefer regulations that empower the end user to screen out harmful content on the receiving end, rather than regulations

ICPA differs fundamentally from COPA's provisions disfavored in *Ashcroft III*. Justice Kennedy suggested that filters were preferable to COPA because "[t]hey impose selective restrictions on speech at the receiving end, not universal restrictions at the source."[276] ICPA *only* restricts users who subscribe to Community Ports—and these Internet users choose the restrictions, just as filter users do. ICPA provides the very advantage Justice Kennedy saw in filters. It allows individual users to "impose selective restrictions at the receiving end, not universal restrictions at the source."[277] All other users will experience the Internet as they always have with no change at all.

Further, Community Ports provide Internet users who want protection with a better option than filters. Indeed, filter failings—including underblocking, private overblocking, cost, limited usage, and circumventability[278]—make filters an inadequate alternative to ICPA.

Even if the Court were to find that ICPA's Open Ports requirement is a universal source restriction, the Court will likely approve the restriction as a reasonable and slight burden. Justice O'Connor in her concurrence in *Reno I* anticipated the "[promising] prospects for the eventual zoning of the Internet."[279] As previously shown, the Court has not left Americans in the real world to the mercy of disruptive speakers who invade personal privacy. The Court's approval of the Do-Not-Call Registry Act, the Pandering Mail Act, home privacy rights in *Hill*, and its "book stack" characterization of Internet offerings in *American Libraries Ass'n* indicates that the Court will approve reasonable laws that prevent others from intruding on private property with unwanted speech.[280]

V. CONCLUSION

A simple change in technology can open new possibilities for addressing the problem of Internet pornography. Because of the Ports Concept's shift from a blanket attempt to prohibit all Internet speech that is Harmful to Minors to a focus on consumer choice of

punishing the content provider for failing to initially screen out harmful content.").

276. *Ashcroft III*, 542 U.S. 656, 667 (2002).

277. *Id.*

278. *See supra* Part IV.B.4 (discussing the shortcomings of filters).

279. *Reno I*, 521 U.S. 844, 891 (1997) (O'Connor, J., concurring).

280. *See supra* Part IV.A.3 (discussing the privacy rights of property owners).

Internet content, ICPA can avoid the constitutional pitfalls that doomed the CDA and COPA. ICPA, as proposed, allows for the unrestricted access to constitutionally protected Internet pornographic material for those who desire it. But it also allows for the receipt of a pornography-free Internet for those who so choose. Such coexistence is crucial to the success of any attempt to allow consumers to determine the nature of Internet content. This simple technological and statutory solution puts the choice to access or to block Internet pornography back in the hands of individuals, where it belongs.