BYU Law Review

Volume 2007 | Issue 6 Article 3

12-18-2007

Making Family-friendly Internet a Reality: The Internet Community Ports Act

Dawn C. Nunziato

Making Family-friendly Internet a Reality: The Internet Community Ports Act

*Cheryl B. Preston**

It is not the critic who counts: [but the one] who is actually in the arena, . . . who strives valiantly, who errs and comes up short again and again, . . . and who, at the worst, if he [or she] fails, at least he [or she] fails while daring greatly, so that his [or her] place shall never be with those cold and timid souls who knew neither victory nor defeat.

Theodore Roosevelt[1]

In many ways, the work of a critic is easy. We risk very little yet enjoy a position over those who offer up their work and their selves to our judgment. We thrive on negative criticism, which is fun to write and to read. But the bitter truth we critics must face is that, in the grand scheme of things, the average piece of junk is more meaningful than our criticism designating it so.

Anton Ego[2]

The February 2007 issue of PEDIATRICS, the magazine of the American Association of Pediatrics, reported that forty-two percent of ten- to seventeen-year-olds in the United States have been exposed to Internet pornography.[3] Of children ages ten and eleven, seventeen percent of boys and sixteen percent of girls have been

* Visiting Professor, S.J. Quinney College of Law, University of Utah; Edwin M. Thomas Professor of Law, J. Reuben Clark Law School, Brigham Young University; 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. Theodore Roosevelt, Citizenship in a Republic, Speech at the Sorbonne, Paris (April 23, 1910).

2. RATATOUILLE (Disney/Pixar 2007).

3. Janis Wolak, Kimberly Mitchell, and David Finkelhor, *Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users*, 119 PEDIATRICS 247, 254 (2007).

exposed to unwanted online pornography.[4] That is the same age that kids learn long division.

Within the last five years, the quantity of pornography, as well as the number of users, has increased exponentially. In August of 2005, Internet users viewed over fifteen billion pages of adult content.[5] This is a positive deluge compared to 1998, during which there were only fourteen million identified pages of pornography.[6] The easy availability of pornography has exploded again as the use of Web-enabled mobile phone and hand-held gaming devices permit the user to surf the Web unfiltered on any wireless signal.[7]

The over twelve-billion-dollar-a-year commercial pornography industry is now being matched, and even overtaken, by free porn and amateur sites[8]—such as YouPorn.[9] "As its name suggests, YouPorn lets users upload and watch a virtually unlimited selection of hardcore sex videos for free. The user-generated clips on YouPorn—like those on YouTube, the site it mimics—range from the grainiest amateur footage to the slickest professional product."[10]

The response to this new Internet "innovation" was astonishing. "Just nine months after going live in September 2006, YouPorn was on pace to log about 15 million unique visitors in May, [2007] . . . and its audience was growing at a rate of 37.5 percent a month.

4. *Id.* at 251, 254.

5. *See* Enough is Enough, Internet Pornography, http://www.enough.org/inside.php?tag=stat%20archives#2 (last visited Jan. 7, 2008) (citing comScore Media Metrix).

6. *See, e.g.*, Press Release, Center for Internet Addiction and Recovery, N2H2 Reports Number of Pornographic Web Pages Now Tops 260 Million and Growing at an Unprecedented Rate (Sept. 23, 2003), *available at* http://www.netaddiction.com/newspr/n2h2_2003.htm; CORPORATION FOR PUBLIC BROADCASTING, CONNECTED TO THE FUTURE: A REPORT ON CHILDREN'S INTERNET USE FROM THE CORPORATION FOR PUBLIC BROADCASTING 4 (2002), http://www.cpb.org/stations/reports/connected/connected_report.pdf ("Children's (ages 2–17) use of the Internet at home increased 68 percent from 2000 to 2002.").

7. *See* Cheryl B. Preston, *WiFi in Utah: Legal and Social Issues*, UTAH B. J., Sept.-Oct. 2007, at 29; Gary Strauss, *Cellphone Technology Rings in Pornography in USA*, USA TODAY, Dec. 13, 2005, at 1D, *available at* http://www.usatoday.com/tech/products/services/2005-12-12-pornography-cellphones_x.htm.

8. 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 (last visited Jan. 7, 2008).

9. YouPorn's "closest competitors" are "Adult Entertainment Broadcast Network's PornoTube and Megarotic, which draws [sic] in users with a limited layer of free videos, then tries to sell premium memberships that offer more content and faster video streaming." *Id.*

10. *Id.*

Today, YouPorn is the No. 1 adult site in the world . . . ."[11] "YouPorn's overall rank[(51)] is higher than CNN.com (84), About.com (114), and Weather.com (195)."[12]

There are no significant barriers to access. David Joseph, the founder of Red Light District, a large porn studio, notes even his eleven-year-old daughter can access the free pornography sites.[13]

The story is that the online amateur pornographers "police themselves" so that problems with child pornography and other illegal content are rare. However, the reporter for Condé Nast Portfolio.com discovered facts that belie this assertion.[14] One morning, a single customer service representative for PornoTube, another free porn video site, "had more than 500 videos to review, most of which had been red-flagged because their descriptions included words such as little boys, force, or rape."[15] Notwithstanding this number, later in the interview, this representative claimed that "the community polices itself."[16] Many parents are quite certain those posting pornography, frequently pictures of themselves engaged in sexual conduct, are not the "community" that should be teaching their adolescents about relationships, the meaning of gender, and the role of sexuality in a healthy life.

In spite of the difficult practical, technical, political, and constitutional issues raised by attempting to protect children on the Internet, responsible government must now confront and deal with them. Acknowledging and solving the problem of children's exposure to Internet pornography becomes more and more imperative with every click, every computer training initiative, and every child who turns eleven. Politicians are looking for proposals

11. *Id.* at 1, 7

12. *Id.* at 7. "Vivid.com, a pay site, is ranked 5,061. . . . [These numbers are a]ccording to Alexa, a website-ranking company . . . . Th[e comparison] numbers are averages for the three-month period from mid-June to mid-September [2007]." *Id.* The updated YouPorn ranking of fifty-one was from November, 2007. YouPorn is ranked first on 100Hot.com for the top one hundred searches for Jan. 7, 2008. Uncensored "Hot List," http://100hot.com/webmkt.hot100/uncensored_top_100_popular_searches.htm (last visited Jan. 7, 2008).

13. Hoffman, *supra* note 8 ("[While these sites generally ask viewers to click that they're over 18, David Joseph admitted,] my 11-year-old could go on at any point."). The younger a child is, the less likely he or she will bother to read the fine print where the age representation may be hidden. Preschoolers now know to just keep scrolling and clicking to get the computer to move forward.

14. *See id.*

15. *Id.*

16. *Id.*

that will work. Those of us who can help—lawyers, wordsmiths, techies, and, especially, those companies who are making a fortune on Internet businesses every day—must start exploring ideas for solutions.

It was once fashionable to write flippant and critical denigrations of the proposals on the table,[17] while slathering on techno-arrogance.[18] It is easy for those who speak of the Web as their personal properry to push back against every change.[19] It is easy to

17. For example, a little ditty on INFO/LAW, a publication began at the Berkman Center for Internet and Society at Harvard Law School where the site is still hosted, reflects the attitude in sentences such as this one:

> [Anti-pornography advocates on CP80.org] claim[] that there are 400 million pornographic Web pages and that, if printed and stacked, they'd be over 15 miles high. (How does this compare to Web pages about kittens and other cute things? Or sports trivia? And how would one store a 15-mile high stack of porn under one's bed? Just thinking.)

Posting of Derek Bambauer to INFO/LAW, *Sandwich Meat, or How Not to Protect Kids from Porn*, http://blogs.law.harvard.edu/infolaw/2007/04/04/sandwich-meat-or-how-not-to-protect-kids-from-porn/ (April 4, 2007). The essay also includes the following response to the definition proposed in ICPA: "Well, it looks like Lego Sex is out on the Community Ports." *Id.* In this sentence, the words "Lego Sex" are a link to an animated video clip showing in detail Lego-built men engaging in sexual activities in a public restroom. This effort to trivialize the discussion, in fact, illustrates the lack of respect for children who might innocently seek Web pages dealing with a favorite toy. Bambauer does not propose an alternative solution.

18. For example, John Barlow—a Wyoming cattle rancher, lyricist for the Grateful Dead, and member of a group of tech-savvy Internet anti-regulationists called the Internet frontiersmen—derided one early governmental attempt to regulate the Internet (the Telecommunications Act of 1996) throngh this Declaration of the Independence of Cyberspace, which captures the general attitude of techno-arrogance:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders.

JOHN PERRY BARLOW, A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE (1996), http://homes.eff.org/~barlow/Declaration-Final.html (last visited April 9, 2007).

19. Internet frontiersmen continue to fight, inter alia, against enforcing copyright law on the Web and the power of government to obtain information to identify cybercriminals, as well as regulations on pornography. *See, e.g.*, Electronic Frontier Foundation, *File Sharing: It's Music to our Ears*, http://www.eff.org/share/ (last visited Jan. 8. 2008); Electronic Frontier Foundation, *History*, http://www.eff.org/about/history.php (last visited Jan. 8, 2008)

insist that no "outsiders"—no one who is over forty, who does not blog, or who does not share music files—could possibly understand the technical complexities of the system sufficient to make a credible proposal for a change in the practices or the architecture of the Internet.[20] It is tempting to believe that nothing can be done.

But American parents are waking up. With their insistence, something must and will be done. The only question is what. The time has arrived to work together to find a reasonable balance among the values of the First Amendment, the appeal of an unfettered technological frontier, and the rights of parents to have the aid of the government in protecting children. My ultimate hope, in putting forth this proposal, is to stimulate the discussion and the innovation necessary to arrive at some solution. I invite all forms of further research, testing, and thinking on the subject.

In this Article, I provide an overview of one such suggestion, the Internet Community Ports concept and the Internet Community Ports Act (ICPA).[21] First, I provide a brief and simple overview of the ICPA's provisions in Part I. Second, I briefly cover a few of the legal issues ICPA is written to address: drawing a definitional line, choosing whether the standard is community or national, defining a minor, identifying and locating offenders, and dealing with unsecured wireless Internet networks.

I. OVERVIEW

A. Introduction to the Legislative Objectives

ICPA is devised to provide nation-wide support for the effective implementation of Internet channeling technology. It balances the constitutional right to freedom of expression and the right to be free from uninvited speech in the privacy of one's private property. This balance allows parents to make meaningful choices concerning their

(declaring that opposition to government subpoenas was one of the catalysts for the founding of the Electronic Frontier Foundation, a corporation devoted to keeping the Internet unregulated); Electronic Frontier Foundation, *Anonymity*, http://www.eff.org/Privacy/Anonymity/ (last visited Jan. 8, 2008) (stating that Internet frontiersmen have "challenged many efforts to impede anonymous communication, both in the courts or the legislatures").

20. In the words of Derek Bambauer, this includes those who propose ICPA, an "approach that's both unconstitutional and technologically moronic." *See* Posting of Derek Bambauer, *supra* note 17.

21. For the full text of ICPA, see *infra* Appendix A.

children's access to sexually graphic material, while still allowing adults to publish and access any legal material online. Terms defined in ICPA are capitalized in the remainer of Article.

ICPA relies on channeling content on various Internet Ports rather than, as is the current practice, sending virtually all content over just a handful of Ports, such as Port 80 for http// browsing and Port 25 for email. The technology for Port channeling already exists, although it has not been employed to give Internet users content choice. The statute empowers an administrative agency to oversee the designation of Ports, process complaints, and conduct preliminary determinations regarding violation of the Act. ICPA is currently written with the Federal Communications Commission (FCC) in that role; but the National Technical and Information Agency (NTIA) of the Department of Commerce has been vested with authority for some other forms of Internet regulation. A switch to NTIA or another body is possible.[22]

Initially, a range of Ports, including Port 80 and Port 25, will be designated as "Community Ports," on which all general use and family content is served. On another range of Ports, designated as "Open Ports," constitutionally protected adult speech may be served. Internet Users who make no change in their connection service will observe no change in their access or use of the Internet. Those who do not want adult material may request from their Internet Service Provider (ISP) a Community Port-only service. With such a service, computer users are unable to access Open Ports. The statute establishes graded penalties for Web Publishers who transmit material Harmful to Minors on Community Ports or who transmit material that is Child Pornography[23] or Obscenity[24] on any Port.[25]

22. Although the NTIA seems like the logical location for the administration of an Internet regulatory scheme, the inclusion of non-commercial actors may require a body outside the Department of Commerce. The subject of jurisdictiou is reserved for another day.

23. New York v. Ferber, 458 U.S. 747, 762 (1982) (holding that child pornography was categorically unprotected speech and defining child pornography as "visual depictions of children performing sexual acts or lewdly exhibiting their genitals").

24. The legal category of "obscenity" is defined in *Miller v. California*, 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 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).

25. *See infra* Appendix A, § III(8)(i), *Penalties.*

The statute also solves problems that have emerged from previous attempts to regulate the Internet.

ICPA requires persons who choose to publish content that is Harmful to Minors to configure their server to direct content over Open Ports, rather than over Community Ports.[26] For those who must occasionally permit Harmful Communications on a Community Port, for a variety of practical reasons such as allowing employees to use remote access to their home computers over which the employer has no control, may choose a second option. This option requires age verification. The burden of age verification is high, but it permits a backup defense for an employer or parent who chooses Community Ports-only service but permits selective Communications subject to the more demanding route of age verification. This exception gives another option to Content Publishers, further lessening the statute's First Amendment implications.

Content served on an Open Port is not altered in any way; the configuration is simple and not visible to those who access the content.[27] ICPA does not prevent any willing adult from speaking or hearing any legal speech. It gives citizens who are not "willing listeners" to pornographic materials the right to not listen, to not let pornographic materials interfere with the way they chose to educate their children, and to not have pornographic materials trespass on their private property.[28] These rights are constitutionally protected.[29] The shift in the approach that allows individual consumer choice serves these important interests and reduces the burden on speech. Now that "turning off our computers" is no longer a viable choice, especially for students, parents need a tool to assist them in making decisions about what their children can access online that is inexpensive, simple, not easily circumvented, and that requires no technological know-how on their part. ICPA may not be the only option ever devised for achieving these goals but it is the one that works and is ready for implementation now.

26. *Id.*

27. *See* Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children* 2007 BYU L. Rev 1417, 1431–34.

28. *See* Ginsberg v. New York, 390 U.S. 629, 639 (1968); Prince v. Massachusetts, 321 U.S. 158, 166 (1944).

29. *Ginsberg*, 390 U.S. at 639; *Prince*, 321 U.S. at 166.

ICPA is a comprehensive scheme addressing detailed mechanics of administration. It includes provisions covering a wide range of issues raised by the problem of Internet pornography. However, many of its provisions could be separated into different stand-alone statutes that would each make significant contributions to solving the problem.[30] Some of these are discussed later in the Article. In addition, some of the particular issues addressed by ICPA could be deferred to state regulation, and some may be reasonably deferred to the rule-making power of an administrative agency. But, because of the size and nature of the Internet, most of the relevant issues are most effectively handled at the federal level.

B. Overview of Provisions

ICPA's provisions follow this basic outline. Many of its provisions could be improved, but its language provides a framework for discussion:

I. **Congressional Findings** of facts and the purposes of the Act.

II. **Prohibition on Harmful Communications.**

1. **Liability of Content Publishers.** Knowingly publishing content that is Harmful to Minors on Community Ports is a violation of the statute. The statute also prohibits publishing material that is Obscene[31] or Child Pornography[32] on any Internet Port. While Obscene material and Child Pornography are already illegal and without constitutional protection, ICPA provides an array of additional mechanisms to assist in enforcement.

30. Provisions that could be valuable on their own include requiring Internet Service Providers to keep records, *see infra* Appendix A, at Part II(4)(i)(a), *Keeps Records*; regulating private wireless connections, *see id.* at Part II(2) *Owners of Private Wireless Connections with Open Port Services*; any or all of the enforcement mechanisms, *see id.* at Part III, *Enforcement*. *See* Cheryl B. Preston, Resources, Legal, State Initiatives 1-5, http://cp80.org/resources/listall, for examples. *See generally* Preston, *supra* note 7 (proposing a Utah statute providing for the mandatory protection of private wireless networks).

31. *See supra* note 24.

32. *See supra* note 23.

2. **Owners of a Private Wireless Connection with Open Port Services.** ICPA requires those who have a wireless Internet network and who subscribe to Open Ports to password protect, filter, or otherwise take steps to insure that Minors cannot use their wireless connection to access pornography on Open Ports. The Act distinguishes between intentionally making wireless access available to Minors and unintentional violations, for which only a small fine can be imposed.[33]

3. **Affirmative Defense of Content Publisher.** ICPA provides an affirmative defense to Content Publishers who transmit Secure Communications.

4. **Affirmative Defenses of Service Providers.** ISPs are not liable as Content Publishers as long as they 1) keep records for two years sufficient to identify the owners of IP Addresses obtained from that ISP; 2) make those records reasonably available for purposes of enforcing the Act and assisting law enforcement; 3) comply with a judicial or administrative Removal Order when a site is found to be in violation of the Act; and 4) reasonably notify customers about when the Act will become effective and about what constitutes a violation of the Act. The Act provides safe-harbor provisions to protect ISPs so they do not risk liability in the course of their Ordinary Service Activities.[34]

5. **Information for Customers.** In order to qualify for the affirmative defenses, a Service Provider must inform its Service Customers of its limitations of liability under the Act.

33. See *infra* Appendix A, § II(2)(i), *Unintentional Access.*

34. *See infra* Appendix A, § II(4)(ii), *Performs only Ordinary Service Activities.*

III. **Enforcement**. Because the Department of Justice is currently overloaded with enforcement of Child Pornography and child abuse statutes, ICPA contemplates a multi-level approach for spreading the responsibility of enforcement. ICPA provides for civil administrative sanctions and for a private civil right of action in appropriate circumstances.

1. **Power of Commission to Administer this Act**. The Act currently designates the FCC to administer the Act, but some other body may be substituted, such as NTIA. As written, ICPA allows the FCC to defer certain responsibilities to those states willing to step up and assist in processing complaints by citizens of that state. States may form State Internet Offices (SIOs) (described below). The deferral provisions are a way to harness the help of those states that are deeply committed to protecting their citizens from the onslaught of pornography.

2. **Notification of Alleged Violation**. Internet users who find Obscene Communications or Child Pornography on any Port or material Harmful to Minors on a Community Port may notify the FCC of an alleged violation of the Act (much like existing procedures regarding indecency in television broadcasts).[35] The Act provides for time limitations and the requirements for an effective Notification, designed primarily to avoid fraudulent and trivial use of the Notification process.

3. **Complaint Procedures**. This section of the statute provides a fairly elaborate procedure for obtaining an administrative determination of whether a certain Internet Communication violares the Act. The Act

35. For an explanation of existing FCC procedures, see *How the FCC Resolves Obscenity/Indecency/Profanity Complaints*, http://www.fcc.gov/eb/oip/flow.pdf (last visited Jan. 7, 2008).

allows for a person who has submitted a Notification to request administrative action (a Complaint Procedure). If a Complaint Procedure is requested, the Content Publisher of the Communication in question is notified, and, following an Initial Determination that the Communication likely violates the Act, the Content Publisher may request a hearing. Following such a hearing, the FCC may make a Second Determination of violation. Either party may appeal such a decision, if made by an State Internet Office, to the FCC. The Enforcement Office may request information regarding the Content Publisher from the records of an ISP in the process of a Complaint Procedure. At appropriate points in this process, the Enforcement Office may issue a Temporary or Final Removal Order to an Internet Registrar, Registry, or ISP for the purpose of removing offending material from the Internet.

4. **Right-to-Sue Letter**. Following a Final Determination that a Communication violates the Act, the person who initiated a Complaint Procedure may obtain permission to seek the civil penalties provided under the Act.

5. **Final Removal Order**. Following the issuance of a Final Determination, the Enforcement Office may issue a Removal Order to have prompt removal, disabling, or blocking the Identified Communication.

6. **Attorney General Enforcement**. The FCC may also request the U.S. Attorney General to enforce the Act.

7. **Jurisdiction**. Any U.S. district court shall have jurisdiction to enforce any Removal Order upon application by the Attorney General.

8. **Civil Penalties and Private Right of Action**. A person with a Right-to-Sue Letter or the Attorney General may bring an action in a U.S. district court

to recover civil penalties for a violation of the Act, following the proceeding described above. The civil penalties vary from $5000 to $100,000 for each violation based on whether the violating Communication is Obscene, Child Pornography, or Harmful to Minors and whether it was made for Commercial Purposes or not. The Act also allows for actual damages and, at the court's discretion, for class actions and punitive damages.

9. **Criminal Penalties.** The Attorney General may seek criminal penalties if an alleged violator intentionally refuses to comply with an order of an Enforcement Office and an order of a district court finding the Communication to be in violation of the statute. A district court may order jail time and forfeiture of equipment, Domain Names, and IP Addresses. In addition, the court may impose a criminal fine in the same amounts of the civil fines described above.

IV. **State Internet Offices**. The state deferral section provides as follows:

1. **Deference to a Qualified State Internet Office.** Certain functions of the FCC may be deferred to SIOs.

2. **State Internet Office Qualifications.** To qualify for such deferral, a state must make a request and show that the state will create a SIO with adequate staffing and funding.

3. **State Internet Office Reporting** An SIO must submit annual and monthly reports to the FCC demonstrating that it is functioning properly.

4. **Withdrawal of Authority**. The FCC can withdraw the authority of an SIO that is no longer qualified to act.

5. **Grants for Funding State Internet Offices**. The Federal Government may provide some funding as an incentive for states to establish SIOs.

6. **Educational Programs of State Internet Offices**. SIOs may also be urged to create Educational Programs to educate parents and children about the risks on the Internet, options for avoiding Internet pornography, and how to assist in enforcement of the Act.

V. **Definitions**. The definitions are sensitive to existing and emerging technology. The statute defines technical jargon and other terms to avoid ambiguity. Many definitions are taken from existing statutes.

VI. **Miscellaneous**. This section contains a severability clause and an effective date of 180 days after enactment.

The possibilities for funding the administration of ICPA are still under discussion. A variety of options exist for providing funding, other than or in addition to congressional appropriations. For instance, an Enforcement Office could charge a small filing fee for a compliant and a larger fee for issuing a Right-to-Sue Letter. ISPs could collect a small fee from those Service Customers who subscribe to the Community Port service and thus choose to avail themselves of the protection of the Act. A small tax on the purchase of handheld Web-enabled devices or wireless routers would generate necessary funds from those most able to absorb the cost, rather than those who purchase the minimal desktop computer and access services.

II. SOME IMPORTANT LEGISLATIVE CHOICES

A. Drawing a Line

1. "Harmful to Minors"

Much of the debate about regulating pornography has stymied on the esoteric impossibility of drawing the line between acceptable

and unacceptable content. However, "definitions" is a diversionary argument. Not only do we know it when we see it, we now have codified the scope of it and relied for federal court purposes on the ready identification of it by a range of observers. Congress has enacted, and the courts have upheld, the definition of "Sexually Explicit Conduct" in various federal statutes, such as 42 U.S.C. § 13031(c)(5), with minimal variations.[36] Even the trade organization for the pornography industry cites the § 13031(c)(5) definition in describing what images it will not include in advertisements submitted for its newsletter.[37]

Of particular interest is the recent Children's Online Protection Act (COPA) case on remand from the Supreme Court to the Eastern District of Pennsylvania. In *ACLU v. Gonzales*,[38] the court freely uses the term "sexually explicit," as well as "adult" and sometimes "harmful to minors," to describe the material covered by COPA's definitions, which Congress intended to protect minors from accessing. In the first paragraph of the opinion, Judge Reed uses "sexually explicit materials" twice,[39] and he uses this phrase again in his "Conclusions."[40] The *Gonzales* Findings of Fact, Section E, is titled, "Sexually Explicit Materials Available on the Web."[41] In that section alone, the opinion uses "sexually explicit" (with the words "material," "Web pages," and "sites") dozens of times.[42] The court summarizes the court-appointed experts' reports filed in the case by describing their findings in terms of "sexually explicit" or "adult" material.[43]

The Findings of Fact were used by the court as reliable evidence of the reach and applicability of COPA. Thus, this opinion, as well as the expert reports relied upon, stands or falls on the ability of the court and the experts to "know it when they see it" and wrap it up in the phrase "sexually explicit," a phrase repeatedly defined in federal law.[44] The experts must have believed that the COPA definitions are

36. *See, e.g.*, 18 U.S.C. § 2256(2)(A) (2000); 15 U.S.C. § 7704(d) (2000); 18 U.S.C. § 3509(a)(9) (2000).

37. *See* Xbiz, http://mediakit.xbiz.com/print.htm (last visited Jan. 24, 2008).

38. 478 F. Supp. 2d 775 (E.D. Pa. 2007).

39. *Id.* at 777.

40. *Id.* at 820.

41. *Id.* at 788 et seq.

42. *Id.* at 789.

43. *See, e.g., id.* at 796.

44. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

easily identifiable and thus legitimately the basis for the precise numerical studies accepted by the court.

Although the *Gonzales* court was truly hostile to COPA, the opinion proves that even critics can understand and apply the COPA definition of "harmful to minors." The *Gonzales* opinion also shows that jurors and Web Publishers can be expected to understand what a definition of "Harmful to Minors" means. This COPA definition incorporates the three prongs of the classic test adopted by the Supreme Court in *Miller v. California*.[45] The Harmful to Minors definition varies from the *Miller* test by asking adult interpreters, such as judges and jurors, to consider the test in light of the interests of Minors, as do the definitions used in *Ginsberg* and COPA.[46] ICPA uses the definition of "Harmful to Minors" from COPA and improves upon it by adding in the second prong, "Sexually Explicit Conduct" from 42 U.S.C. § 13031(c)(5), which provides a more explicit list of depictions for those who need it spelled out. Under ICPA, material Harmful to Minors is "any Communication that:

> i. the average adult, applying a contemporary community standard,[47] would find, taking the Communication as a whole and with respect to Minors, is designed to appeal to, or is designed to pander to, 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; and
>
> iii. taken as a whole, lacks serious literary, artistic, political, or scientific value for Minors.[48]

ICPA's definition is clear and direct, and it represents an easy consensus.

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

46. Ginsberg v. New York, 390 U.S. 629, 638 (1968).

47. For discussion of the community standards requirement, see *infra* Part II.A.2.

48. *See* 47 U.S.C. §231(e)(6)(A)–(e)(6)(C) (2000); 42 U.S.C. § 13031(c)(5) (2000).

2. "Contemporary Community Standard"

In the first Supreme Court appeal of COPA, *Ashcroft v. ACLU* (*Ashcroft I*), the Court ruled on the sole issue of the use of "community standards" in the definition of what is "harmful to minors."[49] The COPA definition was taken from the New York statute upheld by the Supreme Court in *Ginsberg v. New York*,[50] which was based on the Court's definition in *Miller v. California*.[51]

Some commentators prefer a national standard.[52] But the Court has already spoken on the issue of a community standard and it makes sense to stick with language the Court has supported. While a change to a national standard would not invalidate ICPA, a community standard is more appropriate.[53]

Professor John Fee[54] argues persuasively that *Miller*'s[55] and *Ginsberg*'s[56] "community standards" would not result in different First Amendment rights for publishers in different parts of the United States.[57] He explains, "the fact rhat this standard sometimes results in geographic variation is more incidental than it is a matter of constitutional principle."[58] Professor Fee compares the "community standard" to the traditional "reasonable person" test used throughout the law.[59] It allows fact finders to apply a measure that accounts for context and changes in time and place over the life of the law. He concludes:

> Use of an undefined community standard is no more constitutionally problematic in an Internet obscenity case than in any other kind of obscenity case. It is analogous to applying a

49. *See Ashcroft I*, 535 U.S. 564, 585 (2002).

50. 390 U.S. 629 (1968).

51. 413 U.S. 15 (1973).

52. For descriptions of these complaints and accompanying counter-arguments, see John Fee, *Obscenity and the World Wide Web*, 2007 BYU L. REV. 1691, 1713–20.

53. *See Ashcroft I*, 535 U.S. at 587 (O'Connor, J., concurring); *id.* at 591 (Kennedy, J., concurring).

54. Professor, J. Reuben Clark Law School, Brigham Young University. Professor Fee prepared his article *Obscenity and the World Wide Web* for the conference on Pornography, Free Speech and Technology at J. Reuben Clark Law School, Brigham Young University, Feb. 1–2, 2007.

55. 413 U.S. 15 at 24–25.

56. 390 U.S. 629 (1968).

57. Fee, *supra* note 51, at 1691–92.

58. *Id.* at 1692.

59. *Id.*

> "reasonable person" test to a person's business dealings over the Internet: while it is possible that juries in different parts of the country could sometimes apply that phrase differently, it is not designed as a geographically varying standard, and requires no special geographic definition.[60]

Professor Fee further explains that even if Supreme Court precedent provided for geographically varying First Amendment rights, those rights would belong to individual communities, not Web publishers:

> Contrary to popular assumption, the Supreme Court has never held that publishers have a constitutional right to publish according to the standards of their own local vicinage. Nor has it held that publishers have a right to some kind of nationally averaged community standard. In fact, *Miller v. California* squarely rejected this idea, holding that "[i]t is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City."[61]

Finally, Professor Fee argues that using a standard for the Internet that is different from current obscenity jurisprudence, which is based on community standards, "[would] significantly tip the scales in obscenity cases toward defendants."[62] A shift to a national standard would deflect the inquiry away "from a simple question that a juror can answer" using experience, observation, and common sense. The determination would become a "sociological question" requiring expert witnesses and studies, which are "likely to confuse the average juror."[63] ICPA seeks to preserve the diversity of Americans and the rights of individual communities to maintain a level of decency that may have been lost in some central city areas.

3. "Minors"

In *ACLU v. Gonzales*, the court held that COPA was over inclusive because, inter alia, it defined "Minors" as anyone under the age of seventeen.[64] The court feared that, under COPA, Content

60. *Id.*

61. *Id.* (quoting Miller v. California, 413 U.S. 15, 32 (1973)).

62. *Id.*

63. *Id.* at 103.

64. 478 F. Supp. 2d 775 (E.D. Pa. 2007).

Publishers would have to severely restrict their communications because the age test was overbroad. For example, a story that is appropriate for a sixteen-year-old may not be appropriate for an eight-year-old.[65]

The drafters of COPA intentionally chose the age standard that had been reviewed by the Supreme Court in *Ginsberg v. New York*.[66] The Third Circuit's disagreement with *Ginsberg* with respect to age is articulated in *ACLU v. Ashcroft* (*Ashcroft II*), [67] and reiterated by the district court in *Gonzalez*.[68] These courts challenge the existing precedent from the *Commonwealth v. American Booksellers Ass'n*[69] line of cases that empowers courts to interpret this standard as meaning "normal, older adolescents."[70]

These *American Booksellers* cases rely in part on *Pope v. Illinois*.[71] The Third Circuit in *Ashcroft II* finds reliance on *Pope* inappropriate "since nothing in *Pope* implies that where a reasonable minor standard is employed, that the reasonable minor should be considered an older reasonable minor."[72] The precise language in *Pope* is, without question, confusing, seeming to draw what the Court must have perceived as a meaningful distinction between an "ordinary" person and a "reasonable" person.[73] But in context, the *Pope* language is conducive to the interpretation that a reasonable person within the defined group (Minors) is sufficient—thus, a

65. *See id.* at 819.

66. 390 U.S. 629 (1968).

67. 322 F.3d 240, 253–54 (3d Cir. 2003).

68. 478 F. Supp. 2d at 818.

69. 372 S.E.2d 618, 624 (Va. 1989).

70. Am. Booksellers Ass'n v. Virginia, 882 F.2d 125, 127 (4th Cir. 1989) (quoting *Am. Booksellers*, 372 S.E.2d at 624) ("'If a work is found to have serious literary, artistic, political or scientific value for a legitimate minority of normal, older adolescents, then it cannot be said to lack such value for the entire class of juveniles taken as a whole.'"); *see also* Am. Booksellers v. Webb, 919 F.2d 1493, 1508–09 (11th Cir. 1990), *cert. denied*, 500 U.S. 942 (1991); Davis-Kidd Booksellers, Inc. v. McWherter, 866 S.W.2d 520, 527 (Tenn. 1993).

71. 481 U.S. 497, 500–01 (1987).

72. ACLU v. Gonzales, 478 F. Supp. 2d at 817 n.12 (citing *Ashcroft II*, 322 F.3d at 254 n.16 and Am. Booksellers v. Webb, 919 F.2d 1493, 1508–09 (11th Cir. 1990)).

73. *See Pope*, 481 U.S. at 500–01 ("Just as the ideas a work represents need not obtain majority approval to merit protection, neither, insofar as the First Amendment is concerned, does the value of the work vary from community to community based on the degree of local acceptance it has won. The proper inquiry is not whether an ordinary member of any given community would find serious literary, artistic, political, or scientific value in allegedly obscene material, but whether a reasonable person would find such value in the material, taken as a whole.").

reasonable seventeen-year-old mindset can be applied by a juror as the standard. In fact, "reasonableness" in the identified category of Minors is undoubtedly more likely to be an older, more intellectually and socially developed person than a five-year-old.

The court in *Gonzales* justifies the refusal to follow the *American Booksellers* precedent, which allows jurors to presume an older minor under *Ginsberg*-patterned tests, because these cases dealt with hard-copy indecency cases, not the Internet. With hard-copy material, the court argues, the store owner in a face-to-face exchange can distinguish age, but "[t]he Internet merchant has no viable method of determining whether an individual is 6, 12, 17 or 51 years old."[74] The same lack of visual contact with the customer affects all Internet and phone orders. Much hardcopy pornography, especially videos, is now sold over the Internet and mailed to the purchaser. Phone orders or other long distance sales were not uncommon in 1987, when *Pope* was decided, and the Court did not find them a reason to invalidate the "under seventeen" standard. On the Internet, as in other transactions, the seller must presume the customer is underage unless the seller has evidence that the purchaser is of legal age to enter a binding contract. More and more commerce is taking place on the Internet, and sellers of all kinds of goods have found ways to determine if the purchaser can be bound in contract.

In addition, although material suitable for a fifteen-year-old may not be suitable for an eight-year-old, parents arguably have greater control over the activity of eight-year-old children. Similarly, few eight-year-olds are computer savvy enough to hack through an installed filter or creatively explore the Internet. And indeed, material that would arouse a prurient interest in an older teen might pass by many eight-year-olds without a flicker of recognition.

Thus, a more precise articulation of age range is entirely unnecessary under existing law, which assumes jurors have the good sense to apply a reasonable-person-in-the-age-range test. Nonetheless, ICPA, or any other proposed statute, could easily be written to expressly define "Minor" as any person between the ages of thirteen and seventeen.

74. *Gonzales*, 478 F. Supp. 2d. at 818.

B. Appropriate Graded Remedies

Under ICPA, Web publishers who wish to post adult content will configure their Servers with a simple code, like a zip code, that directs such content to Open Ports. This simple Web Server configuration is often accomplished with less than ten lines of code. This setup code is unseen on the screen and has no impact on the content of the material served.

Opponents of pornography regulation stress the supposed chilling effect of criminal consequences for making a wrong call on the legality of marginal speech.[75] Certainly, this was a risk under the CDA and COPA.[76] However, ICPA provides levels of protection to eliminate the risk of inappropriate criminal sanctions.

First, ICPA's definition of Harmful to Minors provides a clearer description of what to avoid than the prior statutes because it incorporates the plain language of 42 U.S.C. § 13031(c)(5). Second, a Content Publisher is entitled to notice of a complaint filed about its Web content, to an administrative hearing, and to an administrative appeal.[77] If the content is found through the administrative process to violate the Act, then an action for civil remedies, rationally scaled to the seriousness of the violation, is available.[78] Only if a Content Publisher knowingly and willfully violates a court order to take down the offending content or repeatedly violates the statute, may the Attorney General bring criminal charges.[79] Because the consequences of an inadvertent violation are so much less draconian (until a Content Publisher refuses to cooperate with a court order or shows a pattern of disregarding the law), ICPA greatly reduces the "chilling" of legitimate speech.

75. *See, e.g.*, PSINet, Inc. v. Chapman, 362 F.3d 227, 235–36 (4th Cir. 2004); ACLU v. Gonzales, 478 F. Supp. 2d 775, 818 (E.D. Pa. 2007) (discussing the chilling effect on free speech imposed by the COPA requirements).

76. *See* Reno v. ACLU, 521 U.S. 844, 872–73 (1997); *Gonzales*, 478 F. Supp. 2d at 818.

77. *See infra* Appendix A, § III(3), *Complaint Procedures.*

78. *See infra* Appendix A, § III(8), *Civil Penalties and Private Right of Action.*

79. *See infra* Appendix A, § III(9), *Criminal Penalties.*

C. Identifying Offenders

Another issue frequently argued by opponents of regulation is the difficulty of tracking down the offenders, who frequently post anonymously or through devices, such as proxy servers, that hide their location and identity.[80] This issue is also overstated. Content Publishers are less hidden than they once were; and those who provide mechanisms for hiding publishers will become responsible for facilitating the distribution of illegal content pursuant to the terms of ICPA.

The definitions of ICPA are written to put responsibility, first, on the Content Publisher who initiates the Communication.[81] But if the Content Publisher cannot be identified because of a failure by another party to comply with the Act, liability falls on those parties that aid in concealing the offender.[82] The definition of a Content Publisher in ICPA is as follows:

> any person who:
>
> i. Transmits, publishes, broadcasts, Posts, Caches, or otherwise uses an IP Address to make or Proxy a Communication; or
> ii. Provides a Link to a Harmful Communication on a Community Port.[83]

ISPs are given a safe harbor as long as they take reasonable steps to preserve a record with respect to the assignment of IP Addresses to customers using the Web—a record that ISPs already generally keep.

1. Proxy sites

One reason that filters are inadequate to protect children is the existence of Proxy technology.[84] One use of Proxy sites is to permit

80. *See, e.g.*, The Electronic Frontier Foundation, https://secure.eff.org/site/Advocacy?cmd=display&page=UserAction&id=301 (last visited Oct. 9, 2007) (arguing that enforcement of government regulation is unfeasible); *see also* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183 (1999) (arguing that government regulation is ineffective and citizens should be left alone).

81. *See infra* Appendix A, § II(1), *Liability of Content Publishers.*

82. *See generally infra* Appendix A, at Part II(4) *Affirmative Defenses of Service Providers.*

83. *See infra* Appendix A, § (V)(12), *Content Publisher(s).*

84. *See generally* MARJORIE HEINS, CHRISTINA CHO, & ARIEL FELDMAN, N.Y.U. SCH.

someone using an Internet filter to route through a Webpage with innocuous content that easily passes the tests of filters. The Proxy then functions to allow the user to retrieve and access material that would be blocked by the filter. Proxy sites also work to hide the user's identity so that the actions of the user on the Internet cannot be easily traced to the actual person. This function is used for anonymity purposes, but is also used to hide cybercrime perpetuators.

Under ICPA a person who elects to set up a Proxy site that permits access to Open Port pornography through a Community Port will be liable, as a Content Publisher, for the material such person makes available on a Community Port.[85] Proxy sites will be subject to the enforcement mechanisms of ICPA, including the power of a court to order the removal of the site from the Web.

2. Hosted sites and Service Providers

Another source of concern is "Hosted" sites on which Posts can be made anonymously or by subscribers who falsify their identity. Host sites are included in the definition of Service Providers.[86] The ICPA definition of Service Providers is as follows:

> any person who is:
>
> i. Providing Internet access;
>
> ii. An Equipment Owner;
>
> iii. A Hoster; or
>
> iv. An IP Address Allocator.[87]

Service Providers, including Hosrers, enjoy the safe harbors similar to those in the Digital Millennium Copyright Act,[88] but a Service Provider may be liable if it fails to keep records sufficient to identify the actual person who Posted illegal content using their

OF LAW BRENNAN CTR. FOR JUSTICE, INTERNET FILTERS: A PUBLIC POLICY REPORT (2006), *available at* http://www.fepproject.org/policyreports/filters2.pdf (discussing the over- and under-inclusiveness of internet filters).

85. *See infra* Appendix A, § II(1), *Liability of Content Publishers.*

86. *See infra* Appendix A, § V(55), *Service Provider(s).*

87. *Id.*

88. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

service.[89] In other words, a Service Provider that fails to keep records for two years sufficient to identify an offending Publisher assumes responsibility for the content itself.[90] Most Hosing sites, such as MySpace and YouTube, have begun to keep records, adopt strict policies, and monitor the content of their sites for compliance with the law. Service Providers typically provide services as a commercial endeavor and, thus, regulation of these commercial activities will be subject only to intermediate First Amendment scrutiny.[91]

One possibility for Service Providers is a scheme of incentives, such as tax breaks for keeping records and assisting with enforcement. The possibility of incentives certainly deserves further consideration. Unfortunately, though, the pornography industry is likely to offer even better incentives, especially economic, than governmental and public interest groups can provide.

3. Service Provider record keeping

The record keeping requirement in ICPA is minimal and consistent with current practices. First, it involves no significant invasion of privacy. It is simply a record of commercial transactions involving the economic-based benefit that is exchanged for the use of an IP Address owned by an ISP. These records are already kept; ICPA only adds a requirement to retain them for a reasonable time to permit law enforcement access during proceedings involving violations of ICPA. An ISPs' complaints about a recordkeeping requirement may represent an interest in appeasing its pornographer customers.

These kinds of requirements are common globally. For example, the European Parliament issued a directive in 2006 setting record retention standard to facilitate "investigation, detection and prosecution of serious crime."[92] The directive requires ISPs to keep certain identifying information for up to two years and make it available to law enforcement officials.[93]

89. *See infra* Appendix A, § II(4)(i), *Cooperation with Enforcement.*

90. *Id.*

91. *See, e.g.*, Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980) (holding that commercial speech is subject to intermediate scrutiny).

92. Council Directive 2006/24, 2006 O.J. (L 105) 54 (EU), *available at* http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/745.pdf (last visited Nov. 28, 2007).

93. *Id.* at 58.

Notwithstanding the mechanisms for finding violators, and ICPA's provisions that discourage others who assist in hiding violators, some violators will no doubt escape prosecution. This is true of every law that exists. It is no reason to simply throw up our hands in despair. The number of U.S. Content Publishers who provide material Harmful to Minors on Community Ports, and Child Pornography and Obscene material on Open Ports, will be significantly reduced. That much would be worth the fight. In addition, a statute in the United States addressing material Harmful to Minors can be enforced in ways that significantly deter international pornographers, in addition to providing strong economic incentives to comply.[94] In any event, ICPA also has mechanisms to have illegal content removed from the Web.[95] The contractual provisions the International Corporation for the Assignment of Names and Numbers (ICANN) requires parties with power to grand access to the Internet root system to honor a court order to remove a site.[96] Thus, even if the offending Content Publisher is not located, Community Port Internet will become a safer place for children and a more productive place for employees.

D. Wireless Internet Access

ICPA requires users who subscribe to an Open Port service and who employ a wireless router to take reasonable efforts to prevent access to pornography through such Wireless Connection" by Minors.[97] Those who install wireless transmitters for their Internet service may use the simple password or other security mechanisms that are available on wireless transmitters as a defense.[98] This provision allows those who subscribe only to Community Ports to protect their children from easily accessing Open Ports over the wireless services of neighboring houses or businesses.[99]

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

95. *See infra* Appendix A, § III(3)(iv), *Temporary Removal Order*; § III(5), *Final Removal Order.*

96. *Id.*

97. *See infra* Appendix A, § II(2), *Owners of Private Wireless Connections with Open Port Services.*

98. For a more extensive explanation and analysis of WiFi issues, see *Preston*, *supra* note 7, at 29.

99. *See id.*

Many minors have cell phones, Blackberries, and other innocent-looking gaming systems, such as Playstation Portable, X-Box 360, and Nintendo Wii, which allow them to access the Internet without filtering.[100] Hundreds of libraries, cafes, parks, malls, and airports offer free wireless Internet access,[101] and hundreds of homes have wireless access that is accessible to strangers if not properly secured.[102] Few parents who go to the bother to install filters and supervise home computer use understand that children can easily access sexually explicit material through a wireless connection at a local fast food restaurant or from their bedroom through a neighbor's unsecured network.

For homes and businesses alike, wireless networks can easily be secured by enabling a password during the set-up procedure. Adding a password is easy, free and smart for several reasons. In addition to protecting minors from pornography, a secured network helps prevent identity theft, credit card fraud, passwords, online crime, and other illegal computer use because activities are traceable.

100. Ordinary gaming systems—i.e., PlayStation Portable (PSP), X-Box 360, and Nintendo Wii—as well as Web-enabled cell phones and Blackberries, for instance, can access the Internet and are available everywhere from around $130 to $500. They do not come with a content filter for minors and they do not have capacity for a filter to be installed. With respect to PSPs, the sales material refers to "Parental Controls." *See* PlayStation Parental Control Levels, http://manuals.playstation.net/document/en/psp/current/settings/parental.html (last visited Nov. 12, 2007). However, this feature only applies to specially programmed universal medium disks (UBD); *see also* PlayStation Technical Specifications, http://www.us.playstation.com/psp/about/techspecs (last visited Nov. 12, 2007). And UBDs are a technology that never caught on. *See* Wikipedia, Universal Media Disc, http://en.wikipedia.org/wiki/Universal_Media_Disc (last visited Nov. 12, 2007). Apparently parents can get an Internet content block on a PSP, but only if they pay for the filter service and buy (and presumably operate) the PSP in Japan. *See* PlayStation, Using the Web Filtering Service, http://manuals.playstation.net/document/en/psp/current/network/browser/Webfilter.html (last visited Jan. 30, 2008).

101. *See* The Wi-Fi-FreeSpot Directory, http://www.wififreespot.com/ut.html (last visited Oct. 24, 2007) (including everything from coffee shops to car dealerships to Burger King).

102. *See, e.g.*, Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, 3–4 (2004) (describing the process of driving through neighborhoods, identifying unsecured wireless access, and marking these locations for others to find and use); Robert McMillan, *Wi-Fi Virus Outbreak is Possible, Researchers Say*, INFOWORLD, Jan. 4, 2008, *available at* http://www.infoworld.com/article/08/01/04/Wi-Fi-virus-outbreak-possible-researchers-say_1.html ("If criminals were to target unsecured wireless routers, they could create an attack that could piggyback across thousands of Wi-Fi networks in urban areas like Chicago or New York City, according to researchers at Indiana University.").

Fines for leaving wireless networks unprotected does not deny any adult the right to use the Internet, set up a wireless network, or access any material, including adult material, thereon. It simply restricts the manner in which one person's decision to have unfiltered wireless access affects others, similar to nuisance laws.[103] Everyone continues to have unfettered access to any Internet service that is not wireless and to any wireless network that is password protected, filtered or subject to any other reasonable means of limiting the unapproved access of Minors to pornography.[104] The simple requirement that wireless networks be either password protected, filtered, or reasonably secured in another way is not burdensome, unconstitutional, or impractical to enforce.[105]

III. CONCLUSION

Finding a workable solution to the problem of underage access to Internet pornography is not as overwhelming as it may seem. Providing a meaningful choice for parents who want to keep pornography out of their homes is one way to protect children from the onslaught of the graphic, and often violent, sexual images readily available online. Defaulting to filters that are over-inclusive, under-inclusive, constantly outdated, and easily circumvented[106] ignores the problem and fails our children. Community Ports are a viable solution because they provide an opt-in choice to Internet users with minimal to no interference with the rights of those who choose to continue accessing legal sexual material by leaving their Internet access service as it currently exists. The technology for zoning the Internet exists. ICPA is written to provide a regulatory framework that allows individual Internet ISP customers a choice at the receiving end of the Internet.

103. *See* Preston, *supra* note 7.

104. *See id.* at 35.

105. *Id.* at 36.

106. Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417, 1450–56.

APPENDIX A

The Internet Community Ports Act of 2007[1]

I. **Congressional Findings**. The Congress finds that:

1. The Internet has become an extremely important and popular means of exchanging information and is relied upon by millions of Americans and other citizens of the globe on a daily basis for personal and commercial purposes. The Internet's global availability makes it extremely convenient and efficient. The Internet plays an essential role in the development and growth of efficient commerce.

2. Many Internet sites contain material that is pornographic, including child pornography, obscene, or inappropriate for children.

3. The availability of Internet pornography to workers on the job costs employers significant numbers of lost work hours, strains employers' computer equipment, reduces productivity, and leads to potentially hostile work environments for both men and women.

4. While the custody, care, and nurture of children resides primarily with the parent, the widespread availability of the Internet presents opportunities for children to access materials in a manner that can defeat the best attempts at parental supervision or control.

5. As children progress through their pre-teen and teenaged years, they begin to use the Internet regularly for school assignments and entertainment. Additionally, around this same age, children experience rapid physical and

1. Drafted by Professor Cheryl B. Preston, Ben Bush, Allan Smart, Ralph Yarrow, the CP80 Foundation, Scott Hilton, Ryan E. Keller, Chris Reed, and numerous volunteers.

emotional development—becoming curious about their own sexuality and beginning to form ideas about sexual relationships. Thus, at this critical stage, many parents may wish to control the effects that Internet pornography can have on their child's developing notions of intimacy and sexual relationships.

6. Some Internet pornographers seek ways to elude filtering programs, target children, and otherwise induce individuals to view or purchase pornographic material.

7. Current methods for protecting computers and computer networks from unwanted Internet content are expensive and negatively affect computer performance. Current methods frequently block more than the intended content. In addition, they are easily circumvented. The cost to deploy such measures, when not prohibitive, consumes both large amounts of money and time. Furthermore, many parents are not adept at procuring and maintaining quality filters.

8. Even if no one ever stumbled unintentionally on pornographic material on the Internet, children and employees may seek out pornography. Warnings and other labels meant to avoid inadvertent hits on pornographic sites may actually lead children to such sites.

9. Notwithstanding the existence of some protections that limit the distribution of pornography over the Internet, there must be continued efforts to protect children from dangers posed by the Internet.

10. It is the policy of the United States to encourage the development of technologies that maximize user control of the Internet.

11. The solution to the rapid growth of pornography on the Internet cannot be solved by law alone; an effective solution requires education, the sensitivity to, use of, and

further development of technological approaches, and the pursuit of cooperative efforts with other countries.

12. While the industry has adopted some self-regulation and developed some innovative ways to help parents and educators restrict material that is inappropriate for children, such efforts have created a false sense of security without providing an effective national solution to the problem of inappropriate material on the Internet.

13. Some states have enacted legislation intended to regulate Internet pornography. These measures cannot be fully successful because of the borderless nature of the Internet.

14. It is the policy of the United States to ensure vigorous enforcement of federal criminal laws to deter and punish trafficking in obscenity, stalking, child pornography, and harassment by means of the Internet.

15. The Department of Justice should continue to use all existing law enforcement tools to facilitate the enforcement of Federal laws, including the tools contained in Title 18 of the United States Code, including specifically, chapters 47 and 63 (relating to fraud and false statements); chapter 71 (relating to obscenity); chapter 110 (relating to the sexual exploitation of children); and chapter 95 (relating to racketeering), as appropriate.

16. Protecting the physical and psychological well-being of children by shielding them from inappropriate materials is a compelling governmental interest.

17. Supporting the right of parents to control the education of their children is a compelling governmental interest.

18. Protecting the right of citizens to control what materials enter their homes and other private property is a compelling governmental interest.

19. Retaining choice and accountability with individuals rather than government is a compelling governmental interest.

20. Preserving the right of free expression embodied in the First Amendment is a compelling governmental interest.

21. The only workable way to address these competing governmental interests is an approach that respects and balances each one.

22. An effective solution to the problem of Internet pornography must respect the First Amendment, provide reasonable protections for children, maximize citizen choice through "opt-in" provisions, accounr for the global nature of the Internet, and encourage technological and economic innovations.

23. The United States Government's partners and resources within the Internet governance community should be called upon to assist in the effort to protect Americans from unwanted Internet pornography.

24. Because of the global nature of the Internet, the fact that a majority of Internet pornography is served from the Unired States and because the United States is a global leader, the United States should create a framework that allows other countries to follow its lead in developing protections for children and that provides economic incentives to guard against Internet abuses.

II. **Prohibition on Harmful Communications.**

1. **Liability of Content Publishers.** A Content Publisher[2] who knowingly and with knowledge of the character of the material, in interstate or foreign commerce:

2. Capitalized terms are defined in Section V *infra*.

i. By means of any Community Port makes or causes to be made any Communication that is Obscene, Child Pornography, or Harmful to Minors;

ii. By means of any Port makes or causes to be made any Communication that is Obscene or Child Pornography,

shall be subject to the penalties described herein. This Section shall not apply to a Service Provider except as provided in Section II(4) and Section III(5).

2. **Owners of a Private Wireless Connection with Open Port Services.**

i. **Unintentional Access.** Any person (including an Internet Service Provider) who uses or deploys a Wireless Connection and fails to take reasonable efforts in good faith to prevent access over such Wireless Connection to a Harmful Communication by a Minor who is not a family member, employee, or guest in a private residence shall subject to a fine as determined by the Commission.

ii. **Reasonable Efforts to Prevent Access.** Reasonable efforts to prevent access to a Harmful Communication on a Wireless Connection include:

a) Requiring a password for access, as long as reasonable efforts are made to prevent Minors from obtaining the password;

b) Filtering Internet access with a commercial filter that is reasonable effective at blocking any Harmful Communication both directly and through the use of a Proxy;

c) Requiring age verification before permitting use of the Wireless Connection, by:

a. Requiring use of a credit card, debit account, adult access code, or adult personal identification number;

b. Accepting a digital certificate that verifies age; or

c. Any other reasonable measures that are feasible under available technology.

iii. **Intentional Access.** Any person who repeatedly violates Section (I), or otherwise makes a Wireless Connection available with intent to permit or cause access by a Minor to a Harmful Communication shall be liable as a Content Publisher pursuant to Section II(1).

3. **Affirmative Defense of Content Publishers.** A Content Publisher who makes or causes to be made a Communication that is Harmful to Minors on a Community Port is not liable pursuant to Section II(1) if such Communication is a Secured Communication.

4. **Affirmative Defenses of Service Providers**. A Service Provider shall not be liable as a Content Publisher pursuant to Section II(1), if it complies with the provisions of this Section.

i. **Cooperation with Enforcement**.

a) **Keeps Records**. A Service Provider keeps a record for two years following any Allocation of an IP Address under its control, excluding Private and Non-Routable IP Address(es), sufficient to reasonably identify:

a. Each IP Address Allocated by or to such Service Provider;

b. The date and time when such IP Address was Allocated; and

c. The IP User who obtained such IP Address;

b) **Provides Records**. Upon receipt of a Notification as provided in Section III(2), a Service Provider makes reasonably available a record as described in Section II(4)(i)(a) to an Enforcement Office;

c) **Controls Access to IP Addresses**. A Service Provider Allocates IP Addresses within its control only to Internet Users who are physically located within the jurisdiction of the United States;

d) **Removes Identified Communication**. Upon receipt of a Removal Order, a Service Provider expeditiously removes, disables, blocks, or otherwise restricts access to the Identified Communication described in such Removal Order; and

e) **Notifies Service Customers**. A Service Provider establishes a reasonable mechanism to notify its Service Customers within sixty (60) days of the enactment of this Act or initiation of access of the following:

a. The effective date of this Act;

b. How to find the definitions used in this Act;

c. How to file a violation report, including contact information for the Commission;

d. How to file a conspicuous statement that:

i. Publishing a Communication that is Obscene or Child Pornography on any Internet Port is illegal;

ii. Publishing a Communication that is Harmful to Minors on a Community Port is illegal;

iii. Upon receipt of such a Communication, the recipient may report it to the Commission and pursue a remedy; and

e. The Service Provider's policies regarding terminating subscriber accounts for violating this Act.

ii. **Performs only Ordinary Service Activities.**[3] A Service Provider is not liable as a Content Publisher pursuant to Section II(1) for conducting Ordinary Service Activities as long as the Service Provider does not:

a) Initiate, Post, reroute, alter, or otherwise take ownership or control of a Communication beyond providing what are common service activities in the industry; or

b) Receive a financial benefit directly attributable to a harmful Communication.

iii. **Removes Identified Communications**. Subject to Section II(5), a Service Provider shall not be liable to

3. These provisions are modeled after the safe harbors in the Digital Millennium Copyright Act (DMCA). *See* 17 U.S.C. § 512 (2000).

an Internet User for any claim based on the Service Provider's good faith action to remove, disable, block, or otherwise restrict access to the Identified Communication pursuant to:

a) A court order issued pursuant to this Act;

b) A subpoena issued pursuant to this Act;

c) A Removal Order; or

d) A Final Determination that there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act.

5. **Information for Customers**. The limitations on liability established by this Section shall apply to a Service Provider only if the Service Provider reasonably informs its Service Customers of the Service Provider's limitations of liability under Section II(4)(iii) through contract or other reasonable means of correspondence.

i. **Designated Agent.**[4] The limitations on liability established in Section II(4)(iii) apply to a Service Provider only if the Service Provider has established a Designated Agent to receive a Notification by making available through its service, including on its website in a location accessible to the public, and by providing to the Commission, substantially the following information:

a) The name, address, phone number, and electronic mail address of the Designated Agent; and

4. The DMCA already requires all ISPs to identify and make available a list of a Designated Agents. 17 U.S.C. § 512(c)(2).

b) Other contact information that the Commission may deem appropriate.

ii. **Directory of Designated Agents**. The Commission shall maintain a current directory of Designated Agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by Service Providers to cover the costs of maintaining the directory.

III. Enforcement

1. **Power of Commission to Administer this Act**. The Commission is empowered, as hereinafter provided, to take action to enforce this Act. The Commission may defer certain responsibilities to a Qualified State Internet Office, as provided in Section IV(1). In addition, the Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its responsibilities under this Act. Not later than 170 days after the date of enactment of this Act, the Commission shall issue regulations to implement the execution of the Commission's responsibilities as described in this Section.

2. **Notification of Alleged Violation.**[5]

i. **Notification**. Upon receipt of either:

a) A Communication on a Community Port that the recipient in good faith reasonably believes is Obscene, Child Pornography, or Harmful to Minors; or

5. These Notification provisions are modeled after the DMCA. 17 U.S.C. § 512(c)(3).

b) A Communication on any port that the recipient in good faith reasonably believes is Obscene or Child Pornography,

the recipient of such Communication (an Aggrieved Party) may file a Notification with either the Commission or a Qualified State Internet Office, if such an Office exists in the jurisdiction where the recipient resides. In addition, the Aggrieved Party may provide a copy of such Notification to the Content Publisher and the Designated Agent of the Service Provider that granted access to the IP Address through which such Communication originated.

ii. **Time for Filing Notification**. If an Aggrieved Party files a Notification that is sufficient under Section III(2)(iii) within ten (10) days following the receipt of such Harmful Communication, the Aggrieved Party will qualify to initiate a Complaint Procedure pursuant to Section III(3)(i).

iii. **Notification Requirements**. To be effective under this Act, a Notification must be a written communication that includes substantially the following:

a) A physical or electronic signature of the Aggrieved Party;

b) Information reasonably sufficient to permit a the Enforcement Office to locate the Communication claimed to be a Harmful Communication, or, if multiple instances of such Communications at a single online site are covered by a single Notification, a representative list of such Communications at that site;

c) The Aggrieved Party's name, street address, email address, and telephone number;

d) A statement that the Aggrieved Party has a good faith belief that the Identified Communication is a Harmful Communication; and

e) A statement, under penalty of perjury, that the information in the Notification is accurate.[6]

f) Such Notification may, but is not required to, include:

a. The approximate date and time when and place where the Identified Communication was received;

b. The URL or IP Address of the Internet site on which the Identified Communication appeared;

c. A statement of reasons why the Aggrieved Party believes the Identified Communication to be a harmful Communication; and

d. A copy or record of the Identified Communication.

3. **Complaint Procedures.**

i. **Initiation of a Complaint Procedure.**

a) **By an Aggrieved Party.** After submitting a Notification to an Enforcement Office as

6. Although the existing enforcement mechanisms for penalizing perjury are sufficient to ensure that few, if any, false Notifications will be filed, a fine could be incorporated for a false claim similar to the $1000 fine for false claims of employment discrimination. For existing penalties for perjury, see 18 U.S.C. § 1621 (2000) (stating that penalties shall last "not more than five years" and include a fine under Title 18 of a minimum of $4000 and maximum of $40,000). Currently, the Commission uses online forms for complaints without mention of penalties for a false complaint, *see* FCC Forms, http://www.fcc.gov/formpage.html (last visited Oct. 18, 2007).

described in Section III(2), the Aggrieved Party may, at any time within a year following the date of such Notification, submit a request to open a Complaint Procedure with respect to the Identified Communication described in the Notification to the Commission or Qualified State Internet Office with which the Notification was filed as provided in Section III(2)(i).

a. Such request must contain information sufficient to identify the relevant Notification, Complainant, Respondent, and Identified Communication.

b. Within thirty (30) days following the receipt of such request, the Enforcement Office shall open a Complaint Procedure with respect to the Identified Communication as described in such Notification.

b) **By the Commission or State Internet Office**. Any time within a year after receiving a Notification as described in Section III(2)(i), the Enforcement Office may open a Complaint Procedure on its own initiative with respect to the Identified Communication as described in such Notification.

ii. **Notifying Respondent of Opening of Complaint Procedure**. Within ten (10) days following the opening of a Complaint Procedure as described in Section III(3), the Enforcement Office shall notify the Respondent of the allegations contained in the Notification and may request additional information concerning the Identified Communication.

iii. **Initial Determination**. Within thirty (30) days after providing notice to the Respondent of the Complaint Procedure in accordance with Section III(3)(ii), the

Enforcement Office shall make an Initial Determination of whether there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act. Following such Determination, the Enforcement Office shall promptly provide the Respondent, and the Complainant if one is involved, with a Notice of Initial Determination.

iv. **Temporary Removal Order.** Following the issuance of an Initial Determination determining that there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act, the Enforcement Office may issue a Temporary Removal Order to the Domain Name registrar, Domain Name registry, other Domain Name authority that registered or assigned the Domain Name, or the Designated Agent of the Service Provider that granted access to the IP Address through which such Communication originated. A Temporary Removal Order may require the prompt removal, disabling, blocking, or other restriction of access to the Identified Communication until a Final Determination can be made. A registrar, registry, Domain Name authority, or Service Provider that fails to comply promptly with a Removal Order shall be liable as a Content Publisher under Section II(1) of this Act.

v. **Administrative Hearing.** The Respondent, and the Complainant if one is involved, shall have thirty (30) days following receipt of a Notice of Initial Determination to request an administrative hearing challenging the Enforcement Office's Initial Determination. The Enforcement Office shall conduct such administrative hearing in accordance with procedures provided by regulations enacted by the Commission in accordance with Section III(1).

vi. **Second Determination**. After conducting an administrative hearing in accordance with Section III(3)(v), the Enforcement Office shall make a Second Determination, either affirming or reversing the Initial Determination. Following such Determination, the Enforcement Office shall promptly provide the Respondent, and the Complainant if one is involved, with a Notice of Second Determination.

vii. **Appeal from a Second Determination of a Qualified State Internet Office**. The Respondent, and rhe Complainant if one is involved, shall have thirty (30) days following receipt of a Notice of Second Determination from an Enforcement Office that is a Qualified State Internet Office to appeal the Second Determination to the Commission.

viii. **Subpoena to Service Provider.**[7]

a) **Request**. Upon initiation of a Complaint Procedure, the Enforcement Office may request the clerk of any United Srates district court to issue a subpoena to a Service Provider for identification of a Content Publisher in accordance with this Section.

b) **Contents of request**. The request may be made by filing with the clerk:

a. A copy of a Notification described in Section III(2);

b. A proposed subpoena; and

c. A sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged

7. This section is based generally on the DMCA. 47 U.S.C. § 512(h).

Content Publisher and that such information will only be used for the purpose of protecting rights under this Act.

c) **Contents of subpoena**. The subpoena shall authorize and order the Service Provider receiving the subpoena to expeditiously disclose to the Enforcement Office information sufficient to identify the alleged Content Publisher of the material described in the subpoena to the extent such information is available to the Service Provider.

d) **Basis for granting subpoena.** If the Notification satisfies the provisions of Section III(2)(iii), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the Service Provider.

e) **Actions of Service Provider receiving subpoena**. Upon receipt of the issued subpoena the Service Provider shall expeditiously disclose to the Enforcement Office the information required by the subpoena, notwithstanding any other provision of law.

f) **Rules applicable to subpoena**. Unless otherwise provided by this Section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

4. **Right-to-Sue Letter**. Following the issuance of a Final Determination determining that there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act, the Complainant may request, and the Enforcement Office shall provide, a Right-to-Sue Letter conferring on the Complainant a private right of action with respect to the Identified Communication to pursue the remedies set forth in Section III(8) of this Act.

5. **Final Removal Order**. Following the issuance of a Final Determination determining that there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act, the Enforcement Office may issue a Final Removal Order to the Domain Name registrar, Domain Name registry, other Domain Name authority that registered or assigned the Domain Name, or the Designated Agent of the Service Provider that granted access to the IP Address through which such Communication originated. A Final Removal Order may require the prompt removal, disabling, blocking, or other restriction of access to the Identified Communication. A registrar, registry Domain Name authority, or Service Provider that fails to comply promptly with a Final Removal Order shall be liable as a Content Publisher under Section II(1) of this Act.

6. **Attorney General Enforcement**. Following the issuance of a Final Determination determining that there is a reasonable likelihood that a court would conclude that the Identified Communication is in violation of this Act, the Commission may request the Attorney General to make application, and the Attorney General is authorized to make application, to a district court of the United States for an order directing immediate compliance with a Removal Order and for remedies as provided herein.

7. **Jurisdiction**. Any district court of the United States shall have jurisdiction, upon application by the Attorney

General, to issue an order directing compliance with a Removal Order and awarding remedies as provided by this Act.

8. **Civil Penalties and Private Right of Action.**

i. **Penalties.** In addition to any other penalties hereunder, a Content Publisher who knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of any Community Port, makes or causes to be made any Communication that is Obscene, Child Pornography, or Harmful to Minors shall be liable for civil penalties to the Commission and, as a private right of action, to any Complainant with respect to such Communication, in an total amount of not more than:

a) $100,000 for each violation by an Obscene Communication or Child Pornography made for a Commercial Purpose; [8]

b) $10,000 for each violation by an Obscene Communication or Child Pornography not made for a Commercial Purpose;

c) $50,000 for each violation by a Communication Harmful to Minors that is made for a Commercial Purpose;

d) $5000 for each violation by a Communication Harmful to Minors that is not made for a Commercial Purpose;

8. Both the criminal and civil penalties are scaled to differentiate both between a Communication that is Obscene or Child Pornography and a communication that is merely Harmful to Minors, and between commercial and noncommercial Content Publishers. The $50,000 fine for a Communication that is Harmful to Minors and made for a Commercial Purpose is set to be the same as provided in the Child Online Protection Act of 1998 (COPA), 47 U.S.C. § 231(e)(2)(A) (2000).

e) Any actual damage sustained by such Complainant as a result of the violation;

f) Punitive damages in such amount as the court may allow;

g) In the case of a class action, such amount as the court may allow, except that the total recovery under this Section in any class action or series of class actions arising out of the same violation by the same Content Publisher shall not be more than the greater of $1,000,000 or one percent of the net worth of the Content Publisher involved; and

h) In the case of any successful action to enforce the foregoing liability, the costs of the action, together with reasonable attorney's fees as determined by the court.

For purposes of this Section, each day of violation shall constitute a separate violation.

ii. **Punitive Damages or Class Action.** For purposes of determining an amount to be awarded as punitive damages or in a class action pursuant to this Section, the court shall consider, among other relevant factors:

a) The amount of any actual damages awarded;

b) The frequency and persistence of failures of compliance by the Content Publisher;

c) The number of Notifications, as provided by Section III(2), or other complaints received by the Content Publisher;

d) The number of Hits accessing any Communication that is the subject of the action;

e) The resources of the Content Publisher;

f) The number of persons adversely affected; and

g) The extent to which the failure of compliance was intentional.

iii. **Jurisdiction**. Any district court of the United States in which a Complainant plaintiff resides shall have jurisdiction over a case brought under this Section.

9. **Criminal Penalties**. Intentional failure to observe a district court order issued pursuant to this Act may be punishable by not more than six months in jail; forfeiture of any equipment, Domain Names, and IP Addresses used in making any Harmful Communication that is the subject of the order; and a fine of not more than:

i. $100,000 for each violation by an Obscene Communication or Child Pornography that is made for a Commercial Purpose;

ii. $10,000 for each violation by an Obscene Communication or Child Pornography that is not made for a Commercial Purpose;

iii. $50,000 for each violation by a Communication Harmful to Minors that is made for a Commercial Purpose; and

iv. $5000 for each violation by a Communication Harmful to Minors that is not made for a Commercial Purpose.

For purposes of this Section, each day of violation shall constitute a separate violation.

IV. State Internet Offices.

1. **Deference to a Qualified State Internet Office**. Any state may create a State Internet Office to assist in the administration of this Act. If a State Internet Office qualifies pursuant to Section IV(2), the Commission shall delegate to such State Internet Office the power to accept Notifications from residents of such state, conduct Complaint Procedures, make Initial Determinations, conduct administrative hearings, make Second Determinations, make Final Determinations, and issue Right-to-Sue Letters with respect to Aggrieved Parties who are residents of such state.

2. **State Internet Office Qualifications**. A state may request the Commission to approve a State Internet Office for deferred administrative assistance pursuant to Section IV(1). Upon such a request, the Commission may determine that such State Internet Office qualifies for deferred administrative assistance by considering the following, in addition to other factors deemed relevant by the Commission:

    i. **Adequate Staffing**. The state must show that the State Internet Office has adequate staffing. Such staffing must include, but is not limited to:

        a) A review board to conduct hearings and make Initial, Secondary, and Final Determinations, singly or in groups, composed of at least five (5) qualified residents of such state. The members of such review board must be able to:

            a. Interpret the definitions and apply the standards provided in this Act in an unbiased and objective manner;

            b. Make fair, careful, equitable, timely, and informed decisions.

b) An administrative staff that is sufficient to enable the State Internet Office to complete the administrative processes outlined in this Act or prescribed by the Commission with reasonable timeliness.

ii. **Adequate Funding.** The state must show that the State Internet Office has, and will continue to have for the year following such request, sufficient funding to enable such State Internet Office to perform effectively the responsibilities delegated to it by the Commission under this Act.

3. **State Internet Office Reporting**

i. **Annual Reports.** All Qualified State Internet Offices shall provide an annual report to the Commission on a date designated by the Commission. The annual report must include:

a) The information required under IV(2) as evidence that the Office continues to qualify for deferred administrative assistance;

b) A chart of the organization of the Office and the agency or authority within the state responsible for the Office;

c) The amount of funds made available by the state to the Office for the purpose of assisting in the administration of this Act;

d) The telephone number(s), location, and identity of the persons responsible for the operation of the Office; and

e) Data on the Office's performance for the prior year, including:

i. The number of Notifications received by the Office;

ii. The number of requests from Aggrieved Parties to open a Complaint Procedure received by the Office;

iii. The number of Complaint Procedures initiated by the Office itself;

iv. The amount of time taken by the Office to complete Complaint Procedures;

v. The number of Communications found by the Office to be Harmful Communications;

vi. The number of Communications found by the Office not to be in violation of this Act; and

vii. All other reasonable information that the Commission deems necessary to make a determination of whether such Office is fit to continue to conduct administrative functions under this Act.

ii. **Monthly Reports**. Each month, on a day designated by the Commission, each Qualified State Internet Offices shall identify all Notifications and requests to open Complaint Procedure received by the Office in the preceding month and the status of each.

4. **Withdrawal of Authority**. If at any time the Commission determines that a previously approved State Internet Office no longer meets the requirements necessary to qualify for deferred administration under this Act, the Commission may withdraw its deferral to such Office.

5. **Grants for Funding State Internet Offices.**

   i. **Commission Grants.** The Commission shall, subject to the availability of appropriations, make grants to states for the purpose of establishing and maintaining Qualified State Internet Offices.

   ii. **Authorization of Appropriations.** Congress is authorized to appropriate $10,000,000 for each of the fiscal years 2007 through 2011 to provide funds for grants as provided in this Section.

6. **Educational Programs of State Internet Offices.**

   i. **Provide Education.** A state that establishes a Qualifying State Internet Office may receive additional funding if the State Internet Office establishes an Educational Program.[9]

   ii. **Coordination.** State Internet Offices may cooperate with and coordinate its Educational Programs with other state and federal programs, such as the DARE program or the public schools system.[10]

   iii. **Curriculum for Educational Programs.**

      a) **Committee on Curriculum.** To qualify for funding, an Educational Programs shall consist of curriculum determined by a Curriculum Committee assembled by the State Internet Office. The State Internet Office has discretion to determine the members of the Curriculum

9. How each State Internet Office would educate could, of course, vary from state to state. Allowing the State Internet Offices of each state to determine how they want to educate allows numerous types of educational interventions. The best types could be disseminated to other State Internet Offices, promoting an effective educational process.

10. The targeted groups could include grade school students to adults. The DARE program serves as a model for how school-based programs could operate. State media efforts such as the recent "Don't DIS-ability" and "Tear off the labels," in addition to anti-smoking and anti-meth campaigns, could serve as media models for state efforts to educate adults about the potentially harmful effects of Internet pornography on a Minor.

Committee, but should consider including individuals with a range of viewpoints and representing:

a. Members of the State Internet Office review board;

b. Local government;

c. The medical community;

d. Academics;

e. Members of local school boards; and

f. Parents and PTA groups.

b) **Recommended Topics.** The Curriculum Committee assembled by the State Internet Office shall have discretion in determining what material to cover in the curriculum created for Educational Programs. Among the topics that the Curriculum Committee should consider are:

a. Risks of early exposure to pornography;

b. Tactics employed by pornographers to attract children to their sites;

c. Penalties for violating this Act;

d. Options for controlling access to unwanted pornography and responding to violations of the Act; and

e. Any other information that the Curriculum Committee determines should be taught as part of the state's Educational Programs.

V. **Definitions**. For purposes of this Act, the following definitions apply:

1. **Aggrieved Party(ies).** The term "Aggrieved Party(ies)" means a person who reasonably believes that he or she has been the recipient of a Communication that is in violation of this Act, but who has not yet initiated a Complaint Procedure.

2. **Alleged Violation(s).** The term "Alleged Violation(s)" means a Communication that is claimed by an Aggrieved Party to be a Harmful Communication, but which has not yet become subject to a Complaint Procedure.

3. **Allocate(s).** The term "Allocate(s)" means distribute, delegate, lease, sublease, grant a license, give, or any other means by which a Service Provider allows another person to use an IP Address.

4. **Caches**. The term "Caches" means utilizing the process whereby an Internet Communication is duplicated or mirrored at an Internet Location other than the location of its origination.

5. **Child Pornography**. The term "Child Pornography" has the meaning given that term in Title 18 Section 2256 of the United States Code.[11]

11. The text of the federal statute referenced is as follows:

(8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where-

(a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. § 2256(8) (2000).

6. **Commercial Purpose(s).**[12] A Content Publisher shall be considered to make a Communication for a Commercial Purpose only if:

   i. Such Content Publisher is Engaged in the Business of making such Communications; and

   ii. Such Communication is made as an advertisement or for the purpose of attracting customers or luring customers to any business enterprise.

7. **Commission.** The term "Commission" means the Federal Communications Commission.

8. **Communication(s).** The term "Communication(s)" includes all Internet Protocol (IP) Packets Transmitted on the Internet and includes all data types and materials. Such data types and materials include text, images, graphics, simulations, animations, video, audio, and other content. A response from an IP Address to any single request for an Internet Communication is considered a separate Communication for purposes of this Act.

9. **Community Port(s).** The term "Community Port(s)" means all Internet Ports that are designated from time to time by the Commission as Community Ports.

10. **Complainant(s).** The term "Complainant(s)" means an Aggrieved Party who has initiated a Complaint Procedure in accordance with Section III(3)(i)(a).

11. **Complaint Procedure(s).** The term "Complaint Procedure(s)" means the process(es) outlined in Section III(3), by which an Enforcement Office determines whether an Alleged Violation is a Communication in violation of this Act.

12. This definition is taken from COPA, 47 U.S.C. § 231(e)(2)(A) (2000).

12. **Content Publisher(s).** The term "Content Publisher(s)" means any person who:

    i. Transmits, publishes, broadcasts, Posts, Caches, or otherwise uses an IP Address to make or Proxy a Communication; or

    ii. Provides a Link to a Harmful Communication on a Community Port.

    With respect to a single Communication, more than one person may be considered to be the Content Publisher.

13. **Curriculum Committee.** The term "Curriculum Committee" means a committee established by a State Internet Office as provided in Section IV(3)(v)(c)(a).

14. **Designated Agent(s).** The term "Designated Agent(s)" means the person(s) selected and identified by a Service Provider to receive Notifications of claimed violations of this Act.

15. **Domain Name(s).** The term "Domain Name(s)" means the text name corresponding to a numeric IP Address of a Server on the Internet.

16. **Education Program(s).** The term "Educational Program(s)" means any program complying with the requirements of Section III(3)(v).

17. **Enforcement Office.** The term "Enforcement Office" means either the Commission or a State Internet Office to which a Notification is sent as described in Section III(2)(i).

18. **Engaged in the Business.**[13] The term "Engaged in the Business" means that the person who makes a Communication, or offers to make a Communication, by

13. *Id.* at § 231(e)(2)(B).

means of the Internet, that includes any Harmful Communication, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such Communications be the person's sole or principal business or source of income). A person may be considered to be Engaged in the Business of making, by means of the Internet, Communications for Commercial Purposes, only if the person knowingly Posts such Communication, causes such Communication to be Posted on the Internet, or knowingly solicits such Communication to be Posted on the Internet.

19. **Equipment Owner(s).** The term "Equipment Owner(s)" means any person who owns equipment that is used to Host or Transmit a Communication on the Internet.

20. **Final Determination(s).** The term "Final Determination(s)" means:

    i. An Initial Determination by either the Commission or a State Internet Office that has not been appealed within the time limits provided in Section III(3)(v);

    ii. A Second Determination made by a State Internet Office that has not been appealed to the Commission within the required time limits provided by Section III(3)(vii);

    iii. A Second Determination made by the Commission; or

    iv. A decision by the Commission made following the appeal of a Second Determination made by a State Internet Office.

21. **Harmful Communication(s).** The term "Harmful Communication(s)" means any Communication that is Obscene, Child Pornography, or Harmful to Minors.

22. **Harmful to Minors.**[14] The term "Harmful to Minors" means any Communication that:

    i. the average adult, applying a contemporary community standard, would find, taking the Communication as a whole and with respecr to Minors, is designed to appeal to, or is designed to pander to, 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; and

    iii. taken as a whole, lacks serious literary, artistic, political, or scientific value for Minors.

23. **Hit(s).** The term "Hit(s)" means a request to a Server including a request from a Web browser or another Web-enabled application for a Communication.

24. **Hoster.** The term "Hoster" means any person who provides Hosting Services.

25. **Hosting Services.** The term "Hosting Services" means providing a Server to Transmit a Communication for a Content Publisher(s).

26. **IANA.** The term "IANA" means the Internet Assigned Numbers Authority.

14. This definition is taken from COPA, 47 U.S.C. § 231(e)(6), with the exception of the phrase "or describes or depicts Sexually Explicit Conduct."

27. **Identified Communication(s).** The term "Identified Communication(s)" means the Communication(s) alleged to be a harmful Communication in a Notification filed with the Commission pursuant to Section III(2)(i).

28. **Initial Determination(s).** The term "Initial Determination(s)" means the first decision in the Complaint Process made by the Enforcement Office that there is a reasonable likelihood that a court would conclude that an Identified Communication is in violation of this Act.

29. **Internet.** The term "Internet" means the combination of computer facilities, transmission media, and related equipment and software, comprising the interconnected worldwide networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP) or a successor protocol to Transmit and receive information.

30. **Internet Location.** The term "Internet Location" means any site, destination, application, data, or other environment that can be accessed by means of the Internet.

31. **Internet Protocol.** The term "Internet Protocol" (IP) means a data-oriented network layer protocol used for communicating data across a Packet-switched network.

32. **Internet User(s).** The term "Internet User(s)" means any person who receives or Transmits any Communication over the Internet.

33. **IP Address(es).** The term "IP Address(es)" means a number that uniquely identifies a device that is connected to a computer network that is Internet Protocol based.

34. **IP Address Allocator.** The term "IP Address Allocator" means any person who Allocates an IP Address.

35. **Link(s).** The term "Link(s)" means a reference to one Internet Location embedded in another Internet Location whereby an Internet User can move directly from one Internet Location to another Internet Location.

36. **Minor(s).**[15] The term "Minor(s)" means any person who is under seventeen (17) years of age.

37. **Notice of Initial Determination.** The term "Notice of Initial Determination" means the notice given to the Respondent, and Complainant if one is involved, of the Initial Determination of the Enforcement Office in a Complaint Procedure.

38. **Notice of Second Determination.** The term "Notice of Second Determination" means the notice given to the Respondent, and Complainant if one is involved, of the Second Determination of the Enforcement Office in a Complaint Procedure.

39. **Notification(s).** The term "Notification(s)" means the formality through which an Aggrieved Party communicates certain facts or events relating to an Identified Communication to the Commission, a State Internet Office, or a Designated Agent.

40. **Obscene.**[16] The term "Obscene" means any Communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that:

    i. the average person, applying contemporary community standards,

15. The designation of a person under age seventeen is taken from Supreme Court language in *Ginsburg v. New York*, 390 U.S. 629, 639 (1968) and *Reno v. ACLU*, 521 U.S. 844 (1997). The "under age seventeen" standard should be interpreted to mean that only those materials inappropriate for a sixteen year old are targeted.

16. This is the traditional definition from *Miller v. California*, 413 U.S. 15, 24 (1973).

ii. would find, taking the material as a whole, is designed to appeal to, or is designed to pander to, the prurient interest;

iii. depicts, describes, or represents, in a manner patently offensive, 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

iv. taken as a whole, lacks serious literary, artistic, political, or scientific value.

41. **Open Port(s).** The term "Open Ports" means all Internet Ports designated from time to time by the Commission as other than Community Ports.

42. **Ordinary Service Activities.** The term "Ordinary Service Activities" means activities typically conducted pursuant to contract by Service Providers on behalf of others who pay fees for such services and are not owned or controlled by the Service Providers. Ordinary Service Activities includes, but is not limited to, Transmitting, routing, providing connections and temporary storage, system Caching, providing storage for a Service Customer, or offering search and location tools.

43. **Packet(s).** The term "Packet(s)" means an electronic container of IP data that is Transmitted via the Internet.

44. **Port(s).** The term "Port(s)" means a number in the Transport Layer data of a Packet identifying either a source or a destination process.

45. **Post(s).** The term "Post(s)" means using a process whereby a Communication enters the Internet (also Posted).

46. **Proxy.** The term "Proxy" means a process whereby an Internet Communication is processed by an intermediary

as a means of masking the identity of any Internet User or permitting access to an Open Port from any device set to receive only Community Ports.

47. **Private and Non-Routable IP Address(es).** The term "Private and Non-Routable IP Address(es)" means the IP Address ranges defined by *Y. Rekhter et al., Best Current Practice: Address Allocation for Private Internets*, RFC 1918 (1996), available at http://www.ietf.org/rfc/rfc1918.txt?number=1918, or any subsequent convention.

48. **Qualified State Internet Office(s).** The term "Qualified State Internet Office(s)" means any State Internet Office that the Commission has determined qualifies for deferred administrative powers pursuant to Section IV(2).

49. **Removal Order(s).** The term "Removal Order(s)" means an order issued by an Enforcement Office following a Final Determination in favor of the Complainaut, requiring the Service Provider to restrict access to the Identified Communication.

50. **Respondent(s).** The term "Respondent(s)" means any Content Publisher responsible for the Identified Communication once a Complaint Procedure has been initiated.

51. **Right-to-Sue Letter(s).** The term "Right-to-Sue Letter(s)" means a document granting a Complainant a private right of action to pursue the remedies provided in Section III(8).

52. **Second Determination(s).** The term "Second Determination(s)" means a decision made by an Enforcement Office following an appeal from an Initial Determination by the Complainant or Respondent, either affirming or reversing the Initial Determination.

53. **Secured Communication.** The term "Secured Communication" means a Communication that is only Transmitted after the Content Publisher, in good faith, has taken reasonable measure to ensure that such Communication cannot be accessed by Minors by:

    i. requiring use of a credit card, debit account, adult access code, or adult personal identification number;

    ii. accepting a digital certificate that verifies age; or

    iii. any other reasonable measures that are feasible under available technology.

54. **Server(s).** The term "Server(s)" means any computer hardware or software that is capable of Transmitting a Communication.

55. **Service Customer(s).** The term "Service Customer(s)" means any person who accesses the Internet using equipment or a Wireless Connection provided by a Service Provider, whether such person pays for the access or not.

56. **Service Provider(s).** The term "Service Provider(s)" means any person who is:

    i. Providing Internet access;

    ii. An Equipment Owner;

    iii. A Hoster; or

    iv. An IP Address Allocator.

57. **Sexually Explicit Conduct.** The term "Sexually Explicit Conduct" has the meaning given that term in Title 42, Section 13031(c)(5) of the United States Code.[17]

17. The text of the federal statute referenced is as follows:

58. **State Internet Office(s).** The term "State Internet Office(s)" means an agency that has been created by a State for the purpose of assisting in the administration of this Act.

59. **Transmission Control Protocol.** The term "Transmission Control Protocol" (TCP) means a Transport Layer protocol used as part of the Internet Protocol stack to facilitate the transmission of data Packets from sender to receiver in a reliable and ordered delivery method.

60. **Transmit(s).** The term "Transmit(s)" means to Post, broadcast, publish, send, or serve a Communication (also Transmitted and Transmitting).

61. **Transport Layer.** The term "Transport Layer" means the protocol layer in the Internet Protocol stack that delivers data to an application process on a computer, such as the TCP and UDP protocols.

62. **Uniform Resource Locator.** The term "Uniform Resource Locator" (URL) includes "Uniform Resource Identifier" (URI) and means a string of characters used to represent and identify resources on the Internet.

63. **User Datagram Protocol.** The term "User Datagram Protocol" (UDP) means a Transport layer protocol used as part of the Internet Protocol stack to facilitate the

---

(5) the term "sexually explicit conduct" means actual or simulated—
(A) sexual intercourse, including sexual contact in the manner of genital-genital, oral-genital, anal-genital, or oral-anal contact, whether between persons of the same or of opposite sex; sexual contact means the intentional touching, either directly or through clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, or arouse or gratify sexual desire of any person;
(B) bestiality;
(C) masturbation;
(D) lascivious exhibition of the genitals or pubic area of a person or animal; or
(E) sadistic or masochistic abuse.

42 U.S.C. § 13031(c)(5) (2000).

transmission of time sensitive, multicast, or broadcast data Packets from sender to receiver.

64. **Wireless Connection.** The term "Wireless Connection" means a method of accessing the Internet using, at any point, electromagnetic waves, rather than some form of wire, cable or other hardware.

VI. Miscellaneous

1. **Default Unprotected Port URI Scheme:**[18] The Commission shall register a URI scheme with IANA defining a default Open Port chosen by the Commission according to *RFC 4395.*[19]

2. **Severability**: If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of this Act and the application of such provision to other persons or circumstances shall not be affected.

3. **Effective Date**: This Act will become effective as of 180 days after its enactment.

18. Designating a "default" Port would eliminate the need for a :<port> at the end of a URL that uses a port other than 80. This approach introduces a new identification scheme (like https). For example "ohttp://example.com" (the o added for "open") would designate the default Open Port chosen by the Commission and registered with IANA instead of Port 80. The registration process is in RFC 4395. Port 81 is currently available, and may be a good choice for the default Open Port. A default secure Open Port (perhaps "ottps") and other parallels within the Open Port range as the Commission deems necessary.

19. T. Hansen, T. Hardie, and L. Masinter, *RFC 4395: Guidelines and Registration Procedures for New URI Schemes*, BEST CURRENT PRAC., Feb. 2006, http://www.rfc-editor.org/rfc/rfc4395.txt.