8 Va. J.L. & Tech. 4 (2003), *at* http://www.vjolt.net

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 2003	8 VA. J.L. & TECH. 4

Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access To Sexually Explicit Content on the Internet?

Russell B. Weekes*

* J.D. candidate, University of Oregon School of Law. Upon graduation, the author will join Reed Data, Inc., a provider of Optical Archiving and Data Storage products, as Director of Operations. The author has spent approximately eight years in the Information Technology industry in various capacities, including technical support, network administration, and web development. The author would like to thank Professor Keith Aoki for his encouragement, Greg Womer for his invaluable comments, and Tiffanie, Preston, Megan, and Emilie for their constant support.

I. Introduction

1. The Internet is arguably the greatest modern-day invention since electricity. The Internet is the printing press, radio, television, telephone, and more rolled-up into one. A vast amount of information on virtually any subject is only a few clicks away. With its incredible potential, the Internet poses unique problems as well.

2. To illustrate, I recently researched automobiles online and requested a brochure from an automaker's website. As a result, I received several e-mail solicitations from local auto dealers. Contemporaneously, I received an e-mail with the subject "air bags." Assuming this was another e-mail from an auto dealer, I uninterestedly opened the e-mail to scan the advertisement before discarding. To my shock, the e-mail contained a jpg[1] image depicting several topless women and explicit cunnilingus, including full frontal nudity and detailed female genitalia. Completely embarrassed and frantic, I quickly deleted the e-mail.

3. As one who finds such material debasing, several thoughts rushed into my mind. What if my five-year old son or three-year-old daughter had seen the e-mail? What if my son was a few years older and *he* had received the mail? What if I had received the e-mail while at work? Could I be fired? What could I have done to prevent receiving this e-mail? What can I do as a parent to prevent my son from receiving such e-mails? As an adult how can I prevent such material from intruding into my home? Why are unwilling inadvertent users exposed to sexually explicit material on the Internet?

4. The above incident is an example of intrusive inadvertent exposure to sexually explicit material ("inadvertent exposure"): I made no deliberate affirmative volitional act to receive the e-mail. Unfortunately inadvertent exposure is neither uncommon[2] nor limited to adults. According to one survey, one in every four minors was inadvertently exposed to sexually explicit material in 1999.[3] Seventy percent of online teens ages 15-17 have been inadvertently exposed to pornography on the web.[4] Perhaps most disconcerting, inadvertent exposure overwhelmingly occurs in the home, but is also frequent at school, or at a public library.[5] When inadvertently exposed to sexually explicit material on the Internet, the user is frequently "mousetrapped"[6] into seeing additional sexually explicit

---

[1] JPEG – or .jpg (after its Windows file extension) – is an image file format frequently used on the Internet.
[2] COMMITTEE TO STUDY TOOLS AND STRATEGIES FOR PROTECTING KIDS FROM PORNOGRAPHY AND THEIR APPLICABILITY TO OTHER INAPPROPRIATE INTERNET CONTENT, NATIONAL RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET § 5.5.2, (Dick Thornburg et al. eds., 2002) [hereinafter COMMITTEE], *available at* http://bob.nap.edu/html/youth_internet/.
[3] *Id*., citing CACRC survey.
[4] Victoria Rideout, *Generation Rx.com: How Young People Use the Internet for Health Information*, pg. 3, (2001), *available at* http://www.kff.org/content/2001/20011211a/GenerationRx.pdf.
[5] 67% at home, 15% at school, and 3% in libraries. See COMMITTEE, *supra* note 2, at § 5.5.2.
[6] Mousetrapping is when a user attempts to leave a website or close the browser and is automatically forwarded to another site. *See* COMMITTEE, *supra* note 2, at § 3.2. Mousetrapping frequently includes a pop-up window, which may result in numerous browser windows being opened. *Id*. Adult site advertisers

material. Thus, the unsuspecting user cannot simply divert her eyes.

5. Inadvertent exposure occurs on the Internet in a variety of ways: spam e-mails; misaddressed e-mails; unknowingly using search terms with sexual and non-sexual meanings as a key word in an online search; [7] adult sites exploiting common misspellings of innocuous sites; [8] confusion between domain names (".com," ".edu," ".gov," etc.); [9] instant messages; [10] and even adult sites replacing former children sites when the domain registration expires,[11] to name the most prevalent.

6. Wide availability, [12] frequent inadvertent exposure by adults and children, the broad array of communication methods, and the invasiveness of the Internet on the home, school and libraries has concerned parents, educators, and politicians searching for solutions to eliminate or ameliorate inadvertent exposure to sexually explicit material on the Internet. Inadvertent Internet exposure poses problems not present in the "real world" because, unlike walking down the street, watching television or listening to the radio, an Internet user cannot simply avert his/her eyes to avoid inadvertent exposure.[13]

7. Part II of this note presents a brief overview of First Amendment limitations on regulating sexually explicit content outside the Internet realm. Part III outlines previous congressional attempts at regulating sexually explicit content on the Internet and their resultant failures. Part IV evaluates potential solutions to the current Internet-sexually-explicit-content issue and argues that a mature domain should be created to isolate such content on the Internet. This note concludes that Internet pornography is a complex problem that requires a complex solution, but that a mature domain is the basis upon which a complete solution should be based because it enjoys the greatest protective value with minimal First Amendment costs.

---

often obtain revenue based on the number of users that they "refer." *Id.* Thus, Mousetrapping is particularly frequent in the online adult industry because it serves as a source of revenue for advertisers. *Id*.

[7] "Beaver" is only one example of a word with a double meaning that would return both non-sexual and sexually explicit websites if used in a search. There are a number of others.

[8] COMMITTEE, *supra* note 2, at § 5.5.2.

[9] For example, www.whitehouse.gov leads to the legitimate government site, but the same name with .com leads to an adult site. Other innocent-sounding URLs that retrieve graphic, sexually explicit depictions include *http://www.boys.com, http://www.girls.com, http://www.coffeebeansupply.com,* and *http://www.BookstoreUSA.com*. *See* Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 419 (E.D. Pa. 2002).

[10] Nicole C. Wong, *Kids Pressed for Sex Online*, WASHINGTON POST, June 20, 2001, at E01.

[11] Susan Stellin, *Pornography Takes Over Financial Site for Children*, N.Y. TIMES, Oct. 26, 2001, at C5.

[12] There are about 400,000 for-pay adult sites globally. *See* COMMITTEE, *supra* note 2, at § 3.1.

[13] Limiting undesired cable channels and channel blocking can eliminate inadvertent exposure on television; The Internet does not currently have an equivalent mechanism to prevent inadvertent exposure. Moreover, a television viewer can change the channel without viewing the television screen by using a remote control, whereas Internet users cannot and are frequently mousetrapped.

II. Obscenity and Indecency Regulations Outside the Internet

8. To understand the permissibility of potential regulations on the Internet, we must first consider potential constraints on governmental action. The foremost legal constraint on potential Internet regulation of sexually explicit material is the First-Amendment right of "free speech."

A. Overview of Obscenity and Indecency

9. The First Amendment states in relevant part, "Congress shall pass no law … abridging the freedom of speech."[14] Not all speech is protected under the First Amendment, however. The Supreme Court has held that "obscenity" is unprotected speech because it is "utterly without social importance.[15] The Court initially struggled to define obscenity, but ultimately concluded that obscenity is a description or depiction of sexual conduct that, taken as a whole, by the average person, applying contemporary community standards: (1) appeals to the prurient interest in sex; (2) portrays sexual conduct specifically defined by applicable state law, in a patently offensive way; and (3) does not have serious literary, artistic, political, or scientific value.[16] Content that meets the *Miller* definition is unprotected by the First Amendment and may be prohibited. The *Miller* definition narrowly defines obscenity to the point that it is generally recognized that only "hard-core" sexually explicit material satisfies the constitutional definition of obscenity.[17]

10. In addition to obscenity, other forms of speech are not fully protected under the First Amendment. That is to say, the speech may be restricted, but not prohibited. In this vein, the Court has permitted regulation of content-based material that does not meet the definition of obscenity, but that infringes on adults' right to privacy.[18] Such restrictions are permitted in at least two instances: (1) when the speech intrudes on the privacy of the home;[19] and (2) when the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure.[20]

11. Furthermore, the Court has recognized an "independent interest in the well-being of its youth."[21] In so doing, the *Ginsberg* Court held that government may

---

[14] U.S CONST. amend I.
[15] Roth v. United States, 354 U.S. 476, 484 (1957).
[16] Miller v. California, 413 U.S. 15, 24 (1973).
[17] COMMITTEE, *supra* note 2, at § 4.1.2.
[18] *See generally,* Rowan v. Post Office Dept., 397 U.S. 728 (1970); Lehman v. City of Shaker Heights, 418 U.S. 298 (1974); Redup v. New York, 386 U.S. 767 (1967).
[19] *Rowan*, 397 U.S. 728.
[20] Erznoznik v. City of Jacksonville, 422 U.S. 205, 212-13 (1975) (holding that prohibiting the display of all nudity of an outdoor theater is unconstitutionally overbroad because the unwilling viewer on a street can avert his or her eyes); *see* Lehman, 418 U.S. 298 (1974) (sustaining a prohibition of political advertisements while permitting non-political advertisements because the degree of captivity and the resultant intrusion on privacy is significantly greater for a passenger on a bus than for a person on the street).
[21] Ginsberg v. New York, 390 U.S. 629, 640 (1968).

prohibit "the sale to minors…of material defined to be obscene on the basis of its appeal to them whether or not it would be obscene to adults."[22] To avoid confusion, the remainder of this note will use "obscenity" to refer to material that may be prohibited under *Miller*, and "indecent" to refer to material that may be restricted from minors under *Ginsberg*. Regulation of indecent material is limited, however. The government may not "reduce the adult population … to reading only what is fit for children."[23] Furthermore, not "all nudity cannot be deemed obscene even as to minors."[24]

1. Child pornography

12. Another facet of protecting children from sexually explicit content is "child pornography." Child pornography is sexually explicit content in which a minor is depicted as engaging in a sexual act.[25] The Court held that child pornography, like obscenity, is unprotected by the First Amendment because it seeks to profit from the sexual exploitation of children.[26] Unlike obscenity, however, *Ferber* held that the state is not required to meet the *Miller* test. Thus child pornography to any degree is prohibited. The Court has upheld statutes that criminalize private possession of child pornography.[27] Possession of obscenity, in contrast, may not be criminalized.[28]

13. A recent decision, somewhat limited the definition of child pornography, however.[29] Child pornography does not include so-called "virtual child pornography," which appears to depict minors but is produced by other means.[30] Virtual child pornography is made using youthful-looking adults or computer-imaging technology.

2. Zoning

14. Zoning ordinances have long been upheld as a means to regulate the geographic location of adult-oriented establishments.[31] Such zoning ordinances are permissible if the ordinance is designed to promote legitimate local zoning interests and focuses on the secondary effects of such establishments.[32] Zoning ordinances of this kind typically limit the geographic location of such establishments to a limited area of the city. In a recent decision, the Court upheld

---

[22] *Id.* at 631.
[23] Butler v. Michigan, 352 U.S. 380, 383 (1957)
[24] *Erznoznik,* 422 U.S. at 213.
[25] The prohibited content involved in child pornography is both the child exposed to sexually explicit conduct and the depiction thereof.
[26] New York v. Ferber, 458 U.S. 747, 758 (1982).
[27] Osborne v. Ohio, 495 U.S. 103, 111 (1990).
[28] Stanley v. Georgia, 394 U.S. 557 (1969).
[29] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
[30] *Id.* This case arose under The Child Pornography Protection Act of 1996 (CPPA).
[31] City of Renton v. Playtime Theaters, Inc., 475 U.S. 41 (1986).
[32] Appropriate secondary effects are generally concerned with crime that is often prevalent near adult-oriented establishments.

a Los Angeles ordinance that prohibited adult oriented establishments within 1,000 feet of each other or within 500 feet of a religious institution, school, or public park.[33]

3. Regulation of Broadcast media

15. Because of broadcast media's invasive nature and the scarcity of available frequencies at its inception, the court has recognized that broadcast media has less First Amendment protection than print material. In evaluating broadcast media, the Court has recognized that "each medium of expression…must be assessed for First Amendment purposes by standards suited to it, for each may present its own problems."[34]

a. Radio

16. In reviewing the constitutionality of restrictions placed on radio broadcasts, the Court has been very protective of children who may inadvertently encounter indecent broadcasts. In *FCC v. Pacifica Foundation*,[35] the Court upheld a prohibition of indecent material on daytime radio. The *Pacifica* court cited two primary reasons for its holding.

17. First, the radio is uniquely pervasive. Unlike communication in the public sphere, radio "confronts the citizen … in the privacy of the home, where the individual's right to be left alone plainly outweighs the First Amendment rights of the intruder."[36] The fact that the radio audience is constantly tuning in and out, and thus that prior warnings cannot completely protect the listener or viewer from unexpected program content, was also recognized.[37]

18. Second, radio is "uniquely accessible to children, even those too young to read."[38] Written material may be "incomprehensible to a first grader, but [the broadcast in question] could have enlarged a child's vocabulary in an instant."[39] Unlike other forms of indecent material that may be restricted at the source,[40] radio cannot distinguish adults from children.

b. Television

19. Similar to radio, courts have been more protective of children in regulating television than in print media. The jurisprudence of television, however, is bifurcated into "over-the-air" television ("television") and cable television

---

[33] City of Los Angeles v. Alameda Books, Inc., 535 U.S. 425 (2002).
[34] Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, at 557 (1975).
[35] 438 U.S. 726 (1978).
[36] *Id*. at 748.
[37] *Id*.
[38] *Id*.
[39] *Id*. at 749.
[40] For example, adult bookstores or adult theaters may prohibit admission to minors.

("cable") regulation.[41] The rationale for treating television differently than cable is that the dual problems of scarcity of channels and the potential for signal interference do not apply in the context of cable. [42]

20. In *Action for Children's Television v. FCC*, [43] ("Act I"), the court applied the FCC's definition of "indecency" as articulated in *Pacifica* to television. Prohibition of indecent programming during times when children are likely viewers was reaffirmed in *Action for Children's Television v. FCC*[44] ("Act II"). Thus under 18 U.S.C. §1464, the FCC may protect children from indecent content for both radio and television during times children are likely to be in the audience.

21. Cable television has offered a broader range of content than television since its inception – including "pornographic"[45] programming. "The less rigorous standard of scrutiny now reserved for [television] regulation … [is] not … extended to cable regulation, since the rationale for such review … does not apply in the context of cable."[46] Indecent programming on cable television is not prohibited. Under Section 505 the Communications Decency Act of 1996 ("§505"),[47] Congress attempted to limit sexually explicit programming, such as Playboy, to times of day when children would most likely not be viewers. The purpose of the Act was to eliminate exposure from "signal bleed."[48] The Court held § 505 unconstitutional because a less restrictive means to accomplish the governmental interest existed: viewers could order signal blocking to prevent signal bleed.[49]

22. In addition, in *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, [50] the Court upheld portions of the Cable Television Consumer Protection and Competition Act of 1992 that provided that cable operators may allow or ban

---

[41] "Broadcast and cable television are distinguished by the different technologies through which they reach viewers. Broadcast stations radiate electromagnetic signals from a central transmitting antenna. These signals can be captured, in turn, by any television set within the antenna's range. Cable systems, by contrast, rely upon a physical, point-to-point connection between a transmission facility and the television sets of individual subscribers. Cable systems make this connection much like telephone companies, using cable or optical fibers strung aboveground or buried in ducts to reach the homes or businesses of subscribers." Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 627-28 (1994).

[42] *Id.* at 622.

[43] 852 F.2d 1332 (D.C. Cir. 1988). The petitioners sought review of an FCC order permitting "indecent broadcast material" only between the hours of midnight and 6:00 a.m. The FCC's previous standard permitted such material from 10:00 p.m. until 6:00 a.m. The court held that there was insufficient First Amendment justification to change the permissive time frame from 10:00 p.m. to midnight.

[44] 932 F.2d 1504 (D.C. Cir. 1991). The court addressed whether a complete ban on indecent programming survived First Amendment protections. The court struck down the FCC's complete ban on indecent broadcasts, reasoning that it was not the least restrictive means to accomplish the governmental interest.

[45] Pornography in this context includes indecent content. It should be mentioned again that obscenity, as defined in *Miller*, is unprotected by the First Amendment. Thus, even in the cable context, obscenity may be prohibited.

[46] *Turner*, 512 U.S. at 622.

[47] 47 U.S.C. §223 (1994 and Supp. IV 1998).

[48] "Signal bleed: is the 'partial reception of video images and/or audio sounds on a scrambled channel.'" Playboy Entm't Group v. United States, 30 F.Supp. 2d 702, 706 (D. Del. 1998).

[49] United States v. Playboy Entm't Group, 529 U.S. 803 (2000).

[50] 518 U.S. 727 (1996).

indecent programming over "leased access"[51] channels.

c. Telephone

23. Restrictions of indecent material over telephone lines must survive a greater level of scrutiny than broadcast media or cable programming. The reasoning for stricter protection is that the telephone is less intrusive on the users; it requires affirmative action on the part of the caller to initiate the call. In *Sable Communications of California, Inc. v. FCC*,[52] the Court struck down portions of Section 223(b) of the Communications Act of 1934.[53] "The statute, as amended in 1988, imposes an outright ban on indecent as well as obscene interstate commercial telephone messages."[54] The court struck down the prohibition of indecent telephone messages in protecting minors because there are less restrictive means for achieving the compelling interest, such as access codes or requiring a credit card.[55]

III. Regulation of the Internet

24. Internet regulation has challenged courts to understand and describe the magnificent technology. In an attempt to describe the characteristics of the Internet, one commentator has analogized the Internet to a story about three blind men and an elephant:

> In attempting to describe the elephant, one blind man embraced the elephant's leg. "It's just like a tree," said the first blind man to his colleagues. "Nonsense," said the second blind man, who was caressing the elephant's trunk. "It's like a great, thick snake." "You are both wrong," exclaimed the third blind man, assaying the elephant's broad flank with both hands. "This elephant is like nothing so much as a huge wall."[56]

25. The analogy illustrates the difficulty in grasping the multifaceted dynamics – e.g., e-mail, newsgroups, world-wide-web, chat rooms, instant messaging, search engines – which the Internet presents.

26. In an effort to find the appropriate First Amendment analysis in the context of the Internet, courts have tried to draw analogies to other media. This has led to what has been dubbed the "battle of analogies."[57]

---

[51] A "leased access" channel is a channel that federal law requires a cable system operator to reserve for commercial lease by unaffiliated third parties. *Id*.
[52] 492 U.S. 115 (1989).
[53] 47 U.S.C. § 223 (2001).
[54] *Sable*, 492 U.S. at 117.
[55] *Id*. at 131.
[56] Eric B. Easton, *Learning Cyberlaw in Cyberspace*, *available at* http://www.cyberspacelaw.org/easton/index.html.
[57] Mark S. Kende, *The Impact of Cyberspace on the First Amendment*, 1 VA. J.L. & TECH. 7 (1997).

A. The Communications Decency Act

1. Overview of The Communications Decency Act

27. Congress' first attempt to regulate children's access to sexually explicit materials on the Internet was the Communications Decency Act of 1996 ("CDA").[58] The day the CDA was enacted into law, the ACLU sought an injunction to prevent enforcement.[59] The ACLU attacked the constitutionality of two provisions of the CDA.

28. First, the ACLU challenged § 223(a)(1)(B), which imposed criminal liability for any person in interstate or foreign communications who, "knowingly … makes, creates, or solicits" and "initiates the transmission" of "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient … is under 18 years of age."

29. Second, § 223(d)(1) ("the patently offensive provision"), makes it a crime to use an interactive computer service to send or display in a manner available to a person under age 18, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."

30. The case was initially reviewed by a three-judge panel[60] and later heard by the Supreme Court.[61] Relying on findings made by the panel, the Court distinguished the Internet from other broadcast media for three reasons: (1) frequencies of communications on the Internet are not limited like television was at its inception; (2) the Internet does not have a history of "government supervision and regulation" like the broadcast industry; [62] and (3) the Internet is "not as 'invasive'" as radio or television.[63] For these reasons, the Court concluded that the appropriate standard of review for Internet speech is strict scrutiny.[64]

31. Applying strict scrutiny, the Court held that the prohibition on transmission of obscene or indecent communications by means of telecommunications device to persons under age 18, or on sending patently offensive communications through use of interactive computer services to persons under age 18 was overbroad (not least restrictive) and thus unconstitutional.[65] Four factors were listed that contributed to the statute's overbreadth. First the CDA's definition of obscenity

---

[58] Telecommunications Act of 1996, 47 U.S.C. § 223(a)-(h) (2001).
[59] ACLU v. Reno, 929 F.Supp. 824 (E.D. Pa, 1996).
[60] The three-judge panel was sitting pursuant to Pub.L. No. 104-104, 110 Stat 56, 561 (note to 47 U.S.C.A. § 223 (1996)).
[61] Reno v. ACLU, 521 U.S. 844 (1996).
[62] *Id.* at 868-69.
[63] *Id*. at 869.
[64] *Id.* at 868-69.
[65] *Id*.

was broader than the definition articulated in *Miller*.[66] Second, current age-verification technology was not an effective method to prevent minors' access to indecent material.[67] Third, the Court relied on the district court's finding that filtering software[68] was a reasonably effective alternative method to prevent minor access to obscene material on the Internet. Finally, the Court expressed reservations about applying contemporary community standards to the Internet.[69]

2. Consideration of the Court's reasoning

32. The Court's reasoning warrants further consideration in several respects. We begin first with the reasoning that the Internet is most like a telephone because it is not as invasive as television. Elaborating on the invasiveness of the Internet, the Court further stated, "[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.' [The District Court] also found that [a]lmost all sexually explicit images are preceded by warnings as to the content, and cited testimony that 'odds are slim' that a user would come across a sexually explicit sight by accident."[70]

33. The author's personal experience detailed above and contemporary studies render this assessment no longer accurate. In November 1998, U.S. Congress mandated a study by the National Research Council ("NRC") to study issues regarding pornography and the Internet.[71] The NRC reported that 25 percent of youth had at least one unwanted exposure to sexual pictures in the year before the survey.[72] Other studies have found that, among teens ages 15-17 who were online, 70 percent say they have accidentally come across pornography on the web and 23 percent of those say it is "very" or "somewhat" often.[73] One in five youth reported receiving a sexual solicitation or approach in the last year, and one in 30 received an aggressive sexual solicitation.[74] The NRC cautions that the figures cited may be underrepresented "because many youth who know that adults are concerned about such solicitations may worry that reporting such incidents could lead to

---

[66] *Id*. at 872-73. The Court noted that the CDA's definition didn't limit by obscenity as it is "specifically defined by the applicable state law." *Id*. at 873. The Court further found that the CDA's definition extended to include excretory activities and organs of both sexual and excretory nature. Furthermore, the CDA's definition did not require that, taken as a whole, the material appeal to prurient interest, and that it lack serious literary, artistic, political, or scientific value. *Id.* at 873.
[67] *Id*. at 876.
[68] Although unspecified, it is highly likely that the Court was referring to filtering software in its discussion of a specific technology that was a reasonably effective alternative that parents could employ to prevent their children from accessing obscene or indecent material.
[69] *Id*. at 873-74. The Court expressed reservations because it felt this would essentially amount to the most conservative community's standards.
[70] *Id*. at 869.
[71] COMMITTEE, *supra* note 2, at viii (Origin of this Study).
[72] *Id*. at 133.
[73] Victoria Rideout, *Generation Rx.com: How Young People Use the Internet for Health Information*, pg. 3. (Dec. 2001), *available at* http://www.kff.org/content/2001/20011211a/GenerationRx.pdf.
[74] COMMITTEE, *supra* note 2, at § 5.4.3.

greater parental restrictions on them."[75] Such staggering statistics can hardly be accurately characterized as "seldom" or "odds are slim." Moreover, the study shows that inadvertent exposure overwhelmingly occurs (67%) while at home.

34. Second, the Court indicated that age-verification online was ineffective. The ineffectiveness is due to the anonymity of the user: a credit card number itself does not identify the actual user, nor does it verify the age of the user. Despite these obvious deficiencies, it is the use of the credit card with an access code that the *Sable* court found as a least restrictive means to prevent minors from indecent telephone conversations. Because the user is anonymous in both contexts, it begs the question why credit card use is sufficiently reliable in the context of the telephone, but not in the context of the Internet.

35. Finally, the Court relied on the district court's finding that filtering software was a reasonably effective alternative method to prevent minor access to obscene material on the Internet. Reliance on such technology is flawed for two reasons. First, the Court was admittedly relying on technology that was not yet widely available.[76] Second, as discussed in section 3 under Filtering Software, *infra*, filtering software is both overinclusive and underinclusive. Such unreliability cannot be characterized as an effective alternative means to prevent inadvertent access to sexually explicit material on the Internet.

B. Child Online Protection Act

36. Congress' attempt to remedy the deficiencies of the CDA was the Child Online Protection Act ("COPA"). In particular, COPA amended 47 U.S.C. §231 to prohibit communication of material that is "harmful to minors" in interstate or foreign commerce via the World Wide Web if it is available to minors. The following changes were made under COPA: (1) the definition of a minor was changed from 18 to under the age of 17;[77] (2) the scope of application was reduced to the World Wide Web rather than the Internet;[78] (3) COPA applies only to commercial sites rather than to commercial and non-commercial sites alike;[79] and (4) COPA prohibits material that is "harmful to minors" rather than "indecent

---

[75] COMMITTEE, *supra* note 2, at n.40.
[76] Reno v. ACLU, 521 U.S. 844, 846 (1997); *contra* ACLU v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002) (holding that filtering software is not a reliable means to restrict material that is harmful to minors because it is both over-inclusive and under-inclusive).
[77] 47 U.S.C.S. § 231(e)(7) (2002).
[78] *See id*. § 231(a)(1).
[79] *See id.* Under COPA, a commercial purpose is found if the site's operator or owner is engaged in the business of making such communications. The phrase "engaged in business" is defined as "the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit or that the making or offering to make such communication be the person's sole or principle business or source of income." *See id.* § 231(e)(2)(A-B).

material."[80] Both the CDA and COPA provide an affirmative defense for defendants who, in good faith, took reasonable measures to restrict access to regulated material – e.g., credit card, debit account, adult access code, or adult personal identification number, or accepting a digital certificate that verifies age.

37. The United States District Court of the Eastern District of Pennsylvania issued a preliminary injunction to prevent COPA's enforcement, [81] which was affirmed by the Third Circuit Court of Appeals.[82] The Third Circuit held that COPA is unconstitutionally overbroad because "the standard by which COPA gauges whether material is 'harmful to minors' is based on identifying 'contemporary community standards'" reduces permissible material to "the most restrictive and conservative state's community standards in order to avoid criminal liability" and because current technology does not permit a web publisher to prevent access to its site based on the user's local.[83]

38. The Supreme Court overturned the Third Circuit's holding, however.[84] In a limited holding, the Court held that applying the contemporary community standard as applied to an Internet regulation was not itself unconstitutional.[85] The case was remanded.

C. Children's Internet Protection Act

39. Congress' attempt to further protect children from indecent material on the Internet while at school or a public library is the Children's Internet Protection Act ("CIPA").[86] CIPA requires schools and libraries that receive federal funds for Internet access from the FCC's E-Rate program,[87] the Department of Education, or the Institute of Museum and Library Services to enforce an Internet safety policy for minors.

40. The safety policy requires application of a "technology protection measure" that "blocks or filters Internet access to visual depictions that are obscene, child

---

[80] The definition of prohibited material was redefined to comport with the *Miller* test. *See id.* § 231(e)(6). Namely, it restricts sexually explicit material if (1) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that the material is designed to appeal to the prurient interests; (2) it 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 or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breasts; and (3) taken as a whole lacks serious literary, artistic, political or scientific value for minors. *Id.*; Miller v. California, 413 U.S. 15 (1973).
[81] ACLU v. Reno, 31 F.Supp.2d 473 (E.D. Pa. 1999).
[82] ACLU v. Reno, 217 F.3d 162 (3d Cir. 2000).
[83] *ACLU*, 217 F.3d at 166.
[84] Ashcroft v. ACLU, 535 U.S. 564 (2002).
[85] *Id*.
[86] 20 U.S.C. § 9134 (West 2002).
[87] The Telecommunications Act of 1996 mandates the E-Rate program. The program establishes a fund, to which phone companies can contribute, that the FCC administers to help finance the wiring of K-12 public schools. Telecommunications Act of 1996, 47 U.S.C. §254(h)(B) (1996).

pornography, or 'harmful to minors.'"[88] CIPA's safety protection measure mandates blocking or filtering of obscenity and child pornography while adults are using the computers.[89] It also mandates blocking or filtering of obscenity, child pornography and indecent material while minors are using the computer.[90] CIPA also allows, but does not require, giving an authorized person the ability to disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.[91]

41. The ACLU sought to enjoin enforcement of CIPA on the grounds that requiring filtering technology was overbroad and unconstitutionally infringed on the First Amendment. [92] In its copious order, the District Court held that CIPA was unconstitutionally overbroad because "given the crudeness of filtering technology, any technology protection measure mandated by CIPA will necessarily block access to a substantial amount of speech whose suppression serves no legitimate government interest."[93] The court found that libraries could implement less restrictive use policies to prevent access and that CIPA's disabling provision was insufficient to cure the constitutional defect.[94]

42. In its order the District Court discusses filtering technology at length, including its functionality, effectiveness, and customization. In assessing the effectiveness of filtering technology, the court concludes:

43. "No presently conceivable technology can make the judgments necessary to determine whether a visual depiction fits the legal definitions of obscenity, child pornography, or harmful to minors. Given the state of the art in filtering and image recognition technology, and the rapidly changing and expanding nature of the Web, we find that filtering products' shortcomings will not be solved through a technical solution in the foreseeable future."[95]

44. It is interesting to note the district court's assessment of filtering technology against the backdrop of *Reno v. ACLU*. As you will recall from above, the Supreme Court found that "[d]espite its limitations, currently available *user-based* software suggests that a reasonably effective method by which *parents* can prevent their children from accessing sexually explicit and other material which the *parents* may believe is inappropriate for their children will soon be widely available."[96] These contradictory assessments of filtering software – within only a few short years – underscore how the court's understanding of technologies related to the Internet has improved.

---

[88] 20 U.S.C. §9134(f)(1) (2003).
[89] § 9134(f)(1)(B).
[90] § 9134(f)(1)(A).
[91] § 9134(f)(3).
[92] Am. Library Ass'n v. United States, 201 F.Supp. 2d 401 (E.D. Pa. 2002).
[93] *Id*. at 489.
[94] *Id*.
[95] *Id.* at 449.
[96] Reno v. ACLU, 521 U.S. 844, 877 (1997) (citing ACLU v. Reno, 929 F.Supp. 824, 842 (E.D. Pa 1996)) (quotations omitted, emphasis in original).

IV. Potential Solutions

45. Commentators, courts, and politicians have articulated several potential solutions ranging from monitoring, *inter alia*, technology-based tools, and infrastructural changes to the Internet. There may be other potential solutions, but because these three potentially offer the broadest protective value, this note will limit discussion to these three.[97] This note evaluates each potential solution for its effectiveness, and potential First Amendment concerns.

46. As we review the constitutionality of these measures, the above analysis indicates that the Court will likely review the measures under strict scrutiny.[98] Thus, the regulation must (1) have a compelling governmental interest; and (2) use the least restrictive means to accomplish the interest.[99]

47. Each potential solution will satisfy the compelling government interest requirement for three reasons. First, the speech[100] intrudes upon an adult's privacy of the home.[101] Second, the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure.[102] Finally, the Court has recognized the "independent interest in the well-being of its youth."[103] Thus, each analysis will address whether the measure is the least restrictive means to advance the compelling governmental interest.

A. Monitoring

48. Monitoring is a measure aimed at preventing youth from accessing sexually explicit material on the Internet.[104] Parents, educators, and librarians in a variety of ways can monitor a child's use of the Internet including direct observation,[105] viewing the browser's history,[106] cached files,[107] cookies,[108] remote monitoring,[109]

---

[97] One suggested solution is to prohibit spam (unsolicited) e-mails containing sexually explicit material. While this solution may be appropriate and effective, its protective value is very narrow. For this reason, it is not evaluated in-depth in this note.
[98] ACLU v. Reno, 929 F.Supp. at 869.
[99] *Id.*
[100] The "speech" in this context is exposure to sexually explicit content.
[101] *See, e.g.,* Rowan v. Post Office Dept., 397 U.S. 728 (1970); Lehman v. City of Shaker Heights, 418 U.S. 298 (1974); Redrup v. New York, 386 U.S. 767 (1967).
[102] Erznoznik v. City of Jacksonville, 422 U.S. 205, 213 (1975) (holding that prohibiting the display of all nudity of an outdoor theater is unconstitutionally overbroad because the unwilling viewer on a street can avert his or her eyes); *See* Lehman, 418 U.S. 298 (1974) (sustaining a prohibition of political advertisements while permitting non-political advertisements because the degree of captivity and the resultant intrusion on privacy is significantly greater for a passenger on a bus than for a person on the street).
[103] Ginsberg v. New York, 390 U.S. 629, 640 (1968).
[104] COMMITTEE, *supra* note 2, at § 12.2; *Am. Library Ass'n*, 201 F.Supp. 2d at 401.
[105] This is often accomplished by locating the computer in a conspicuous location such as near a librarian station or in a location of high traffic in the home.
[106] Each browser tracks recently visited sites. A savvy user, however, can delete the browser's history, rendering history tracking ineffective.

keystroke capturing,[110] and reviewing e-mail.

49. First Amendment concerns in connection with monitoring may arise if a monitor[111] restricts minors from accessing material that is not indecent. A second potential concern is if monitors attempt to restrict adult access to indecent material.

50. As mentioned above, changing the location of a computer may be sufficient to implement such a measure. Educators and librarians are already charged with monitoring the activities of their constituents. Because of its simplicity and limited First Amendment implication, courts and commentators alike have favored monitoring as a solution to children's access to online sexually explicit material.[112]

51. While courts and commentators may initially favor monitoring to solve the "youth-exposure-to-sexually-explicit-material-problem," extreme caution is warranted. It is readily apparent that monitoring is not a mechanism to prevent inadvertent access to sexually explicit material; monitoring only has a deterrent effect.[113] The threat of "being caught" deters youth from *intentionally* accessing sexually explicit material.[114] While, monitoring may be an effective deterrent from intentional access of sexually explicit material on the Internet, it is a wholly ineffective preventative measure. Monitoring inadvertent access may afford a "teaching moment" to discuss the content with the user, but the damage has already taken place: the child has already been held captive by unwillingly exposure. From a protective position, the primary concern must be to *prevent* inadvertent access. Thus, monitoring is an unacceptable solution to exposure of sexually explicit content on the Internet.

---

[107] Each time a user visits a website, the graphics displayed on the website are generally cached (saved) in a folder on the user's machine to accelerate future access to the webpage. Again, a savvy user can delete cached images cover her tracks.

[108] "Cookies" refers to a file saved to the user's computer that is written by the website developer to store information about the user such as whether the user has visited the site previously. Cookies also may be deleted by the user. *See* http://www.iopus.com/starr.htm.

[109] Remote monitoring refers to technology that permits the host computer to view that which is displayed on the client's monitor. An example of such software is pcAnywhere. *See* http://www.symantec.com/pcanywhere/Consumer/.

[110] Keystroke software records the keystrokes on a given computer, thus allowing a monitor to determine if the user is searching for or accessing sexually explicit material.

[111] The First Amendment issue regarding monitoring only arises in the context of schools and libraries; parental monitoring is likely outside the purview of First Amendment protection.

[112] *Am. Library Ass'n*, 201 F.Supp.2d at 425-27. Note, *Is COPPA A Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests On the Internet*, 28 FORDHAM URB. L.J. 1831.

[113] COMMITTEE, *supra* note 2, at § 12.2.

[114] The effectiveness of monitoring is questionable in a practical sense because savvy users can frequently circumvent detection, particularly because youth users are often more adept computer users than the monitors (parents, educators and librarians).

B. Self-Regulation by the Adult Entertainment Industry

52. Another regulatory theory that has minimal First Amendment impact is allowing the adult entertainment industry to self-regulate. Some commentators argue, explicitly and implicitly, that the adult entertainment industry can effectively self-regulate out of fear of congressional regulation.[115] Such measures include encouraging users to report offensive material by prominently displaying an icon[116] and enforcing ISP terms of service, which prohibit users from posting or sending inappropriate material, harassment, or other inappropriate behavior.[117]

53. If self-imposed, these measures likely have little First Amendment implication.[118] While these measures each provide some positive protection, without additional measures they do not have broad-scope preventative value.[119] They should not be relied on alone, but should be implemented in conjunction with other broader-scope prevention measures.

54. An important self-regulatory broad-scope preventative measure is removing sexually explicit teaser images.[120] Teaser images are placed on the site's homepage as a means to advertise the site's content. This measure would prevent inadvertent exposure to sexually explicit material when the user mistypes a URL, enters a site that did not previously contain sexually explicit content,[121] or unknowingly selects a site from a search engine that contains sexually explicit material. This measure may also prevent intentional access as well.[122]

55. Reliance on the adult entertainment industry to remove teaser images of their own volition is misplaced, however. The adult online industry is highly saturated and relies on aggressive marketing that is antithetical to self-regulation altogether.[123] Furthermore, survey indicates that about 74 percent of adult-oriented commercial

---

[115] *See* COMMITTEE, *supra* note 2.
[116] Offending material would likely be limited to material that meets the *Miller* standard of obscene material and child pornography.
[117] *See, e.g.*, COMMITTEE, *supra* note 2, at § 9.6.
[118] Legislative measures that prohibit posting or sending sexually explicit material may have First Amendment problems. Posting or sending indecent (harmful to minors) may not be constitutional when the same posting or sending is also sent to adults. *See* Am. Libr. Ass'n v. U.S., 201 F.Supp.2d 401 (E.D. Pa. 2002). Moreover, obscenity may be defined differently in the originating state from the receiving state, unless there is a national community standard applied.
[119] For example, using contract law to prevent transmission or posting of sexually explicit material [narrowly applies] to users who might otherwise be exposed while in a chat room. This would not apply to inadvertent visits to other chat rooms, sites with sexually explicit content, spam e-mails, direct file transfers such as peer-to-peer, and others. Thus, the protective value is very narrow.
[120] Teaser images are images that are placed on a homepage and do not require the user to login before accessing sexually explicit content.
[121] The content of a website is subject to change at any time. In addition, domain name registration must be renewed. Content additions and change of domain name ownership are examples of how a previously visited website's content may contain sexually explicit content at subsequent visits.
[122] If a website requires one to login prior to displaying sexually explicit material, children who seek out sexually explicit material will be less able to access sexually explicit material.
[123] COMMITTEE, *supra* note 2, at § 3.3.

sites display sexually explicit content on their first page, which is available to anyone who accesses the site.[124] Moreover, most adult sites offer a free preview to sexually explicit material.[125] Teaser images and free previews are a means to advertise the site's content. Industry actors are unlikely to participate in a removal effort because so doing would exacerbate their economic struggles. Even if all adult sites removed teaser images, there is little reason to believe that site operators would not continue offering a free preview.[126] Thus, the unintentional effect of preventing inadvertent access in this way would continue to promote intentional access.

56. Another popular self-regulating measure that addresses both inadvertent and intentional access is to have website operators self-rate the content of their site. The rating system is analogous to a movie rating system; it is "quasi cyber-zoning." The rating would be included in a meta-tag,[127] which could be used by search engines and users to avoid access to sites with certain ratings. Accompanied with filtering software, the user could prevent inadvertent exposure to sexually explicit material by unknowingly selecting an adult site from a search engine, misspelling the URL of an innocuous sites, using the wrong domain name (".com," ".edu," ".gov," etc.) and other means of accessing adult sites. In addition, a rating system would reduce or eliminate overblocking and underblocking because filtering software could screen the meta-tag and deny access to sites whose rating exceeds a predefined or user-defined threshold.

57. The First Amendment may not apply to a rating system applied to all websites if it is successfully argued that the regulation is not content-based.[128] The purpose of the regulation, however, is to distinguish appropriate/inappropriate content. Thus the *application* of the rating system *is* content based. At any rate, even if the First Amendment applies, a rating system does not prevent adults from accessing protected material (indecent) nor would minors be prevented from accessing material that is not indecent. In this way, a rating system does not restrict protected speech and should survive constitutional challenge under the First Amendment.

58. The weaknesses of a self-rating system begin with its genesis. Who would devise the rating system? What if some actors in the industry do not participate? While some commentators believe that self-regulatory approaches can be successful because "firms in an industry are generally willing to abide by a common code of

---

[124] COMMITTEE, *supra* note 2, at § 3.3.
[125] *Id*.
[126] *Id.*
[127] A meta-tag is a multi-purpose HTML tag that is placed in the header of a webpage. A meta-tag's function includes describing the content of the page (used in search engines), providing key words to match search queries, and preventing the page from being cached, among other things. *See* CONTROLLING SEARCH ENGINE INDEXING WITH THE TAG (1997), *available at* http://www.microsoft.com/technet/archive/default.asp?url=/technet/archive/ie/maintain/etn9764.asp.
[128] If the rating system is applied to all sites, it would not implicate the First Amendment because the measure would not be "content" based.

behavior,"[129] one must question whether such a theory has any basis in reality.

59. First, participation is optional; because the measure is self-regulation there is no mandatory enforcement. Second, economic pressures run counter to self-regulatory measures. When weighing economic pressures against self-regulation, it would be no small miracle for adult entertainment firms to choose self-regulation. To be sure, if industry actors are willing to self-regulate, why have they not done so to-date? Based on the legislation that we have reviewed, Congress is obviously willing to act. Why, then, have "willing" industry actors not asserted themselves and done so? The reality is that the fear of potentially more intrusive regulation is not a sufficiently compelling impetus for industry action; the economic pressures are greater.

60. A *mandatory* rating system, however, may be workable. Congress could establish the system and provide civil and/or criminal penalties for industry actors who fail to adequately rate their site. A mandatory rating system would be a step in the right direction because of its broad protective value and effectiveness as described above.

61. One downside to a rating system is that the onus is on the user to purchase filtering software to prevent inadvertent exposure.[130] Without a second technology to read the rating and screen based on a threshold, a rating system does little to prevent access. Second, metadata is not indelible. Adding, changing, and deleting a rating to a webpage is as easy as changing a meta-tag. Thus, it would be very difficult to ascertain violations, making enforcement somewhat problematic.[131]

C. Technology-based prevention Tools

62. Technology-based tools have been the source of hope to remedy the sexually explicit material on the Internet since Congress has attempted to regulate the Internet.[132] There are many mutations of different technology-based prevention tools, but the most frequently discussed are software-filtering programs and age verification technology.

1. Filtering Software

63. Software filters allow inappropriate Internet activities or material to be blocked. Determination of inappropriate content can be made by the technology, human judgment, or a combination of the two.[133] In general a software filter employs an algorithm to "test" the appropriateness of the activity or material. The algorithm

---

[129] COMMITTEE, *supra* note 2, at § 9.6.
[130] It is possible that a web browser's security settings would effectively serve as filters. If this were to be the case, additional filtering software would be unnecessary. Since web browsers are generally free, users would bear no cost to use the rating system.
[131] Placing an icon with a hyperlink to report violations could improve enforcement of a rating system.
[132] Reno v. ACLU, 521 U.S. 844 (1996).
[133] COMMITTEE, *supra* note 2, at § 2.1.

may be a predetermined by comparing a site to good/bad site lists, by real-time analysis of content or a combination of the two. Exact algorithms vary from developer to developer. Generally filtering software employs one or more of the following filtering methods.

64. First, filters screen sites based on domain names or IP addresses.[134] This is based on predefined lists of good (white lists) and bad (black list) sites. Black lists are lists of sites that are deemed inappropriate, and that the user is prevented from accessing.[135] White lists are lists of sites that are deemed appropriate, and that the user is allowed to access.[136]

65. Relying exclusively on predetermined lists is problematic. First, the lists are not static; new sites are constantly coming online and content on old sites change frequently. For reliable efficacy, the lists must be updated constantly.[137] Second, screening based on IP addresses does not prevent spam e-mail or other real-time communications. Finally, both black lists and white lists suffer from overblocking and underblocking.[138]

66. Second, labels can be used as a means of filtering inappropriate content. Meta-tags (metadata) can contain information about the website. Metadata includes a description of the site and search terms. Search engines index results based on the search terms or keywords. Search engines often arrange index results based on the number of times the word(s) in the query appear(s) on the site. Thus, "extended repetition of commonly used search terms in the metadata, which have no relationship to the actual content of the site itself, will result in that site being retrieved and placed highly in the results when those terms are used."[139] Thus, metadata is often inaccurate.

67. Third, filtering software uses textual analysis. Textual analysis examines of all the text on a site or page and compares the text against a list of words that are

---

[134] The Internet is organized by IP addresses, which identify websites in a manner roughly analogous to finding a street address. Because remembering a series of numbers is more difficult than a name, each IP address has a corresponding domain name to identify a website. Either the IP address or a domain name can be used to access a particular website. When the domain name is used, domain registries resolve the domain name to the corresponding IP address.

[135] "The research indicates that products that employ human verification of black lists tend to be the more accurate in blocking offensive content, and are less likely to block access to suitable content. Filters of this type are likely to be more suitable for families with older children, with requirements to access a broader range of content." AUSTRALIA BROADCASTING AUTHORITY, *Report on Effectiveness of Internet Filter Software* (Mar. 26, 2002), *available at* http://www.aba.gov.au/abanews/news_releases/2002/25nr02.htm [hereinafter ABA Report].

[136] "'[W]hite lists' are the most efficient at blocking offensive content, as they allow users to access a preselected set of sites that have been assessed for their suitability. However, as a consequence, they also block a significant amount of content that may not necessarily be offensive." *Id*.

[137] Software filters that analyze textual content may update black and white lists when a user accesses a site.

[138] *See* ABA Report, *supra* note 135.

[139] COMMITTEE, *supra* note 2, at § 2.1.

strongly associated with inappropriate content.[140] For example, words like "nudity," "sex," "beaver," "breast," etc. may be blocked or flagged for inappropriate content. Words, however, often have multiple meanings. Filtering software has difficulty distinguishing between sexual and nonsexual connotations. For example, "beaver" has both sexual and nonsexual meanings. Filtering software often attempts to identify phrases like "beaver dams" to avoid screening out ("overblocking") sites that are appropriate, but such methods are imperfect. Moreover, filter software also doesn't screen some inappropriate sites for various reasons ("underblocking"), including where the site only has images and doesn't include text.[141]

68. Sexually explicit content is almost always associated with images.[142] Determining the content of an image is virtually impossible. Filter developers have attempted to identify "large expanses of what is likely to be flesh in an image" in an attempt to screen inappropriate images. Such technology, however, is "highly error-prone."[143]

69. Attempting to minimize underblocking and overblocking, software filter developers have tried to classify or categorize the text based on the text as a whole by analyzing the statistical ratio of appropriate words against inappropriate words to screen sites.[144] Even with classification, however, software filters suffer significantly from both underblocking and overblocking.[145]

70. In sum, all filtering software programs suffer from overblocking and underblocking.[146] It is the overblocking and underblocking that raises serious First Amendment concerns in filtering software. Thus, software-filtering programs, without more, cannot currently be viewed as a legitimate preventative measure to protect inadvertent access to sexually explicit content on the Internet.[147]

2. Age-verification

71. Age-verification tools are often suggested as solutions to prevent children's access to sexually explicit content on the Internet. In the physical word, presenting a credential that contains a reliable date of birth (e.g., driver's license or birth certificate) frequently verifies age. Face-to-face communication helps

---

[140] COMMITTEE, *supra* note 2, at § 2.1.
[141] This was the case, as you will recall, in the unsolicited e-mail sent to the author described in the introduction. *See* Am. Libr. Ass'n v. United States, 201 F.Supp.2d 401 (ED Pa. 2002).
[142] *Id*.
[143] COMMITTEE, *supra* note 2, at § 2.1.
[144] *Id.* at § 2.3.1.
[145] *Am. Libr. Ass'n*, 201 F.Supp. 2d at 406.
[146] COMMITTEE, *supra* note 2, at § 2.3; *Am Library Ass'n*, 201 F.Supp. 2d at 410; *See also* ABA Report, *supra* note 135; Bobbi Nodell, MSNBC, *Filtering Porn? Maybe, Maybe Not* (Aug. 9, 2000), *available at* http://www.msnbc.com/news/438174.asp; David McGuire, WASHINGTON POST.COM, *Laws, Internet Filters Not Enough to Protect Kids Online* (May 2, 2002), *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A23527-2002May2&notFound=true.
[147] *See Am. Library Ass'n*, 201 F.Supp. 2d at 427-32.

ensure that the person presenting the credential matches the identity of credential offered (driver's license pictures matches the person presenting the driver's license).

72. Credit cards,[148] JavaScript,[149] and digital certificates,[150] are methods employed in an attempt to verify the user's age on the Internet. In the virtual world of the Internet, ensuring that the credential matches the user is very difficult indeed. Internet users are by in large anonymous. Thus, even if the credential verifies the age reliably, it does not verify the user.

73. Furthermore, age-verification attempts to verify adulthood (generally 18), but the age of adulthood differs from state to state.[151] Thus, if a state defines adulthood at age 16, and a website denies access because the user is not 18, First Amendment issues arise.

74. Finally, even if a reliable age verification technology existed it would not address inadvertent access of sexually explicit material; it would only prevent intentional access.[152] For these reasons, implementing age-verification tools is not a reliable solution. Age-verification technology, however, could compliment other preventative measures.[153]

---

[148] This is a particularly popular method of age-verification on the Internet because credit cards are generally the method of payment. COMMITTEE, *supra* note 2, at § 2.3.2. The method is predicated on the assumption that many adults have a credit card while minors generally do not. *Id*. "Taken in the large, this is not a bad assumption – the vast majority of credit cards are in fact owned by adults, and the vast majority of minors do not own or have legitimate access to credit cards. Thus, an adult-oriented Web site that uses credit cards as its medium of exchange presumes that the presentation of a valid credit card also verifies that the card user is of legal age." *Id*. However, "the imposition of such a requirement would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material." Reno v. ACLU, 521 U.S. 844, 856 (1997). Some age verification services ("AVSs") add additional protection by validating the user's personal information against public records such as driver's license and/or voting records that contain or imply age information. *Id.* When adult status is confirmed, the AVS will mail a password (via postal service) to the address of record on the public record, thus ensuring that the credentials provided match the user presenting the credentials.

[149] JavaScript is a programming language used to ask the user a series of questions about her age, date of birth, etc., to verify age. The obvious problem with this method is there is no mechanism to verify the veracity of the user's responses.

[150] Digital certificates are used to validate the user and her personal information. The problem with relying on digital forms of verification, again, is that there is no way to determine who is actually using the computer that supplied the certificate. If an adult has a certificate on his home computer, for example, and his children have access to the computer, it remains difficult to verify the user. Requiring a password at the time of supplying the certificate is one possible solution to the unverifiable user problem, but again, this solution is not perfect.

[151] COMMITTEE, *supra* note 2, at § 13.3.2.

[152] Age-verification would not prevent inadvertent access if teaser images were still on the homepage.

[153] Age-verification combined with restricting sexually explicit teasers is a potential solution with broad protective value. Its limitations are that inadvertent exposure via spam e-mail, peer-to-peer file transfer, chat-rooms, and instant messaging would still not be addressed.

D. Infrastructural Changes

75. Websites on the Internet are generally identified by a domain name: .com for commercial sites, .edu for educational sites, .mil for military sites, .gov for government sites, etc. Domain names are both functional and informative, and are also used to indicate a country's jurisdiction.[154] Just as domain names are used to identify a government site, a TLD could be established to identify sites with sexually explicit content ("mature domain")[155] or create a child-friendly domain ("kid's domain"). An infrastructural change that creates a mature domain on the Internet is "cyber-zoning."

76. Creation of a kid's domain does not enjoy broad-scope effectiveness that a mature domain does. Kid's domains would limit content on the domain based on the appropriateness for children. In effect, the content would be "especially for kids." Such a domain would not include all material that may otherwise be appropriate to older teenagers. Thus, if children were limited to a kid's domain, they would be excluded from potentially valuable information – particularly older teens. If kids did visit a non-kids-domain site, the same problem that we currently have would apply to those sites. For these reasons, a kid's domain is deficient and is not discussed in depth in this note.

77. Some argue participation in a mature TLD could be either voluntary or mandatory.[156] For the same reasons delineated under adult industry self-regulation of this section, the system must be mandatory to enjoy full benefits of a TLD solution, however. A mandatory system is possible by requiring indecent material to be issued a mature domain name.[157] Currently, some TLDs (".edu," ".mil," ".gov,") are limited to entities whose eligibility to obtain the TLD is determined by an adjudicative body.[158] Eligibility to those domain names, however, is not content-based. A mature domain necessitates establishing an adjudicative body to review the websites content and determine whether the site should be required to

---

[154] For example, ".as," ".au," ".ca," ".jp," and ".uk" are country-code identifiers that are administered by country-code managers. In June 1998, the U.S. Government White Paper, recognized that national governments have a role in "manag[ing] or establish[ing] policy for their own ccTLDs." Internet Corporation for Assigned Names and Numbers ("ICANN"), *ccTLD Resource Materials*, *available at* http://www.icann.org/cctlds/ (last visited Jan. 31, 2003).

[155] The number of TLDs is virtually infinitely expandable. In 2000, ICANN approved seven new TLDs: ".aero," ".biz," ".coop," ".info," ".museum," ".name," and ".pro."

[156] *See* COMMITTEE, *supra* note 2, at § 13.1.

[157] This could be accomplished by exposing site operators to civil and/or criminal liability for sexually explicit content that meets the legal definition of indecency that does not reside on a mature domain. Application of a mandatory mature domain would likely require an adjudicatory body that reviews website content. *See* COMMITTEE, supra note 2, at § 13.1.3. The authors also indicate that establishing an adjudicating body may present difficulties because it would raise the issue of which community standard the adjudicating body would apply. Since the time this article was written, however, the Supreme Court has held that applying a community standard on the Internet is not itself unconstitutional. Ashcroft v. ACLU, 535 U.S. 564 (2002). Moreover, Justices Breyer and O'Connor advocate the desirability of adopting a national standard. *Id* at 586-593. (O'Connor, J., Breyer, J., concurring).

[158] COMMITTEE, *supra* note 2, at § 13.1.1.

use a mature domain name.[159] Sites with content meeting or exceeding the *Miller* definition of indecency would be required to obtain a mature (".mat") domain name.[160]

78. The benefits of a mature domain are broad. A matures domain enjoys preventative value for unknowingly using search terms with sexual and non-sexual meanings as a key word in an online search, [161] adult sites exploiting common misspellings of innocuous sites,[162] confusion between domain names (.com, .edu, .gov, etc.),[163] and even adult sites replacing former children sites when the domain registration expires without requiring filtering software. [164] In addition, it affords *users* a simple way to recognize sites with sexually explicit material to further prevent inadvertent access. Exposure from spam or misaddressed e-mails[165] is also easily accomplished because the user can readily see the .mat domain name in the sender's e-mail address.

79. Furthermore, a mature TLD would ameliorate intentional access by minors because filtering software could eliminate access to all adult sites based on the domain name. A mature domain may also eliminate the constitutional deficiency of mandatory filtering software. By zoning all sites that are indecent, accuracy of filtering software is improved as well. [166] Software filters could key on the domain

---

[159] Domain names are currently issued by registrars accredited by Internet Corporation for Assigned Names and Numbers ("ICANN"). *See*, Internet Corporation for Assigned Names and Numbers, *About ICANN*, *available at* http://www.icann.org/general/abouticann.htm (last visited Jan. 31, 2003).

[160] Others have suggested using ".xxx" to identify a mature TLD. There is a certain amount of stigma attached to XXX, however, to which some "soft-core" sites may object. To ameliorate potential stigma associated with a mature TLD, ".mat" should be the domain used. Also note, "obscene" material is not constitutionally protected and can be prohibited from any site within U.S. jurisdiction. Again, the author agrees with Justices O'Connor and Breyer that Congress should establish a national standard as applied to the Internet so as to give clarity to the definition for the benefit of both the adjudicative body charged with its application and website operators.

[161] Users would not have to rely on the website operator's description or keywords – which are often misleading – to determine if the site contained sexually explicit content because the domain name would be ".mat."

[162] Again, the user would not inadvertently access the adult site because the domain name would easily identify the site as containing sexually explicit material.

[163] Based on the example in the introduction, www.whitehouse.gov leads to legitimate government site, but the same name with .com leads to an adult site. Under a mature domain TLD infrastructure, "www.whitehouse.com" would be changed to "www.whitehouse.mat," which can be easily identified as an adult site.

[164] This phenomenon would be prevented completely because adult sites would be required to have a ".mat" domain name.

[165] E-mails coming from an adult site would have the domain name ".mat," which can be easily screened or deleted without viewing the content.

[166] There is some ambiguity as to whether a mandatory TLD would apply to international websites. *See* COMMITTEE, *supra* note 2, at § 13.1.2. Courts, however, have exerted general jurisdiction when a foreign defendant has "substantial" or "continuous and systematic" activities in the forum state or specific jurisdiction over foreign websites that are "interactive" and have persistent contacts. *See, e.g.,* Panavision Int'l v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) (holding that jurisdiction was appropriate because defendant engaged in tort-like scheme to register company's trademarks as domain names in order to extort money from company and directed that conduct toward the forum); Blumenthal v. Drudge, 992 F.Supp. 44 (D.D.C 1998) (exerting jurisdiction because defendant regularly distributed his column electronically to

name to establish black/white lists, thereby significantly improving – if not eliminating – overblocking and underblocking of sexually explicit material.

80. There are incentives for the adult online industry to support a mature domain infrastructure because adult site operators want their sites to be found and placing their site on a domain devoted to adult-oriented material improves the user's ability to locate the site.[167] Indeed, industry actors acknowledge, "a concentration of adult-oriented Web sites may in fact provide … adults with a target-rich environment in which they could much more easily seek out sexually explicit material."[168]

81. A mature domain is a content-base restriction and must therefore pass First Amendment muster. Because a mature domain applies to the Internet, the likely standard of review is strict scrutiny.[169] Thus the regulation must (1) have a compelling governmental interest; and (2) use the least restrictive means to accomplish the interest.[170] As analyzed at the beginning of this section, creating a mature domain is a compelling governmental interest. Thus we turn to whether it employs the least restrictive means to accomplish that interest.

82. A mature domain does not restrict protected speech under the First Amendment. Protected speech that a mature domain implicates is indecent speech. The test is whether adults would be prevented from accessing indecent speech or minors would be prevented from accessing speech that is not indecent. Under a mature domain infrastructure, adults are not restricted from accessing indecent speech. So long as the *Miller* definition of indecent (harmful to minors) is used to distinguish mature material, a mature domain would not infringe on First Amendment protected speech.

83. Moreover, a mature domain name infrastructure likely improves software-filtering technology sufficiently to survive constitutional challenge when used in schools and libraries. Children using a computer in schools or libraries can be prevented from accessing mature sites through the use of improved software filters. So long as libraries and schools allow adults to bypass blockage of indecent material,

---

local residents, solicited and received contributions from local residents). Thus, a mandatory TLD would likely apply to international commercial websites that have U.S. resident subscribers. Given the economic landscape of adult online industry, there is little reason to suppose that international site operators would avoid servicing U.S. residents in an effort to avoid mature domain requirements. Nevertheless, for international websites who do not wish to have a mature domain and are willing to forgo servicing U.S. residents, there are several options at the disposal of site operators. First, since 1998, the U.S. has recognized that national governments have a role in "manag[ing] or establish[ing] policy for their own ccTLDs." Internet Corporation for Assigned Names and Numbers, *ccTLD Resource Materials*, *available at* http://www.icann.org/cctlds/ (last visited Jan. 31, 2003). Legislation could afford an affirmative defense for international sites that have a ccTLD that do not intend on servicing U.S. residents. Second, international sites can utilize contract terms to prevent U.S. residents from subscribing to their site.

[167] COMMITTEE, *supra* note 2, at § 13.1.2.

[168] *Id.* (quotations omitted).

[169] ACLU v. Reno, 929 F.Supp. at 869 (E.D. Pa, 1996).

[170] *Id*. at 855.

legislation similar to CIPA would no longer be unconstitutionally overbroad.

84. A mature domain, does not address all aspects of inadvertent access of sexually explicit material on the Internet, however. It does not address instant message communications, peer-to-peer file transfers, and chat rooms. Prevention of inadvertent exposure to sexually explicit content arising in connection with one of these methods requires additional safeguards. Thus, a mature domain is not a "cure-all."

85. A mature domain, however, prevents minors' inadvertent and even intentional exposure to sexually explicit content better than any other single measure. Because of its broad-scope preventative value and compliance with First Amendment jurisprudence, legislators should seriously consider legislation mandating a mature domain.

V. Conclusion

86. The Internet poses challenges to courts, parents, and politicians that do not arise in the physical realm--particularly in dealing with sexually explicit content and the First Amendment. Internet users (adults and children) are frequently held captive by inadvertent exposure to sexually explicit content. Such exposure most frequently occurs in the privacy of one's home, but also occurs in schools and public libraries. Under the current Internet landscape, adults and children are unable to prevent such invasive exposure.

87. Preventing exposure to sexually explicit material on the Internet is a compelling interest because the "speaker" of such material invades adults' privacy of the home; it is impractical for the unwilling viewer or auditor to avoid exposure; and there is an independent interest in protecting the well-being of children.

88. Initially, courts have been hesitant to uphold governmental regulations on the Internet, however. In part, their reluctance was based on a misunderstanding of technology. With a greater understanding of the Internet and potential solutions, recent developments indicate that the Court is more willing to uphold Internet restrictions. Advocates and commentators are becoming more adept in finding solutions that deal with the Internet as well.

89. Sexually explicit content on the Internet is a complex problem. Potential solutions must balance governmental interests with First Amendment protections. Some have suggested that no governmental regulation is required because parents, educators, and librarians can simply monitor and educate children. While monitoring and education are important measures in dealing with sexually explicit material on the Internet, reliance solely on these measures ignores the impact of inadvertent exposure and the rights of adults and children to be free from such exposure.

90. Others have suggested that the "adult" industry can successfully self-regulate. The

current adult Internet industry landscape, however, indicates that reliance on the industry to self-regulate is misplaced. Perhaps the strongest measure of self-regulation is a rating system (quasi cyber-zoning). A rating system offers strong preventative value, but would be more effective if the system was mandatory and administered by a governmental agency. A rating system, however, places the onus on the user to purchase additional software so as to prevent inadvertent access to sexually explicit material because the user cannot readily view a site's rating. Moreover, a rating system does not prevent inadvertent exposure to sexually explicit e-mail, chat room communications, and instant messages.

91. Still other solutions are technology-based. Filtering software and age-verification are two such measures. Under the current infrastructure on the Internet, however, filtering software is both overinclusive and underinclusive. The overinclusiveness and underinclusiveness make filtering software neither a reliable solution for parents, nor a constitutional measure for legislators. An age-verification measure is an ineffective solution to the problem without other significant measures. Its constitutionality is also in question.

92. Finally, infrastructural changes offer the broadest protection to inadvertent and even intentional access to sexually explicit content on the Internet. The best infrastructural change is creating a .mat TLD. A mature TLD prevents most inadvertent exposure to sexually explicit material; it does not prevent exposure to sexually explicit content communicated via instant messages, file transfers, or chat rooms, however. Thus, no one solution will "cure" the Internet problem.

93. The complex problem of exposure to sexually explicit content on the Internet requires a complex solution. Initially, the measure with the greatest protection without restricting adult access to content protected by the First Amendment is creating a mature domain. Legislators should seriously consider mandating a mature domain.