UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 3
Issue 2 *Spring 2002*

Article 7

3-1-2002

Keeping Children from the Internet's Red Light District: Increased Regulation or Improved Technology

Angela M. Xenakis

Comment: Keeping Children from the Internet's 'Red Light District': Increased Regulation or Improved Technology?

Angela M. Xenakis[1]

I. Introduction

The Internet has revolutionized the world by providing virtually unlimited access to information and by creating a new medium for social interaction. While extremely advantageous, this unlimited access to information also leads to children being exposed to potentially harmful, sexually explicit material. With its vast number of sites, it is estimated that the World Wide Web contains more than one billion different Web pages.[2] Approximately fifteen million of these pages have pornographic content.[3] With this many sites, access to pornographic websites is only one click away, whether intentional or not. For example, if one accidentally types 'whitehouse.com' instead of 'whitehouse.gov,' one will end up at a pornographic website offering a free trial membership.[4]

[1] J.D. Candidate 2003, University of North Carolina School of Law.
[2] Web Myths & Hoaxes: The Web is Overrun with X-Rated Sites, *at* http://websearch.about.com/internet.websearch/library/myths/bl_xsites.htm (last visited Dec. 31, 2001) (on file with the North Carolina Journal of Law & Technology).
[3] *Id.* Dr. Steve Lawrence and Dr. Lee Giles, researchers at the NEC Research Institute, conducted a study that indicated approximately 1.5% of all web pages contain pornographic content.
[4] *See* Whitehouse.com main page, *at* http://www.whitehouse.com (last visited Feb. 17, 2001) (on file with the North Carolina Journal of Law & Technology).

By the year 2005, forty-four million children under the age of eighteen are expected to be using the Internet.[5] As children's access to the Internet and the number of websites continue to grow, there is continual debate over what, if anything, should be done to shield children from these pornographic sites. Congress has repeatedly and, to date, unsuccessfully tried to regulate access to these sites by children. The debate centers on how best to protect children from pornography without violating free speech rights guaranteed in the First Amendment. In the end, the best solution may come from market forces and new technology instead of laws, since the unique nature of the Internet makes it extremely difficult to regulate.

II. Constitutionally Protected Free Speech

While some may believe that pornography is the ultimate bastion of free speech protected by the First Amendment, the Supreme Court has ruled otherwise.[6] The Court has often struggled over the definition of obscenity; however, it has not moved away from the principle that obscenity is not protected speech and therefore can be regulated. In *Miller v. California*, the Court stated that it "recognized that the States have a legitimate interest in prohibiting the dissemination or exhibition of obscene material when the mode of dissemination carries with it a

[5] News Release, Grunwald Associates, Children, Families and the Internet (June 7, 2000), *available at* http://www.grunwald.com/survey/newsrelease.html (last visited Dec. 31, 2001) (on file with the North Carolina Journal of Law & Technology).

[6] Roth v. United States, 354 U.S. 476 (1957) (holding that obscenity is not within the area of constitutionally protected speech or press).

significant danger of offending the sensibilities of unwilling recipients or of exposure to juveniles."[7]

Miller outlined a three-prong test for what constitutes obscene material, which requires that (1) an "average person applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interests"; (2) the "work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law"; and (3) the "work taken as a whole, lacks serious literary, artistic, political, or scientific value."[8]

In *Ginsberg v. New York*, the Supreme Court allowed analysis based on a different standard when the regulations were directed at protecting children. In *Ginsberg*, the Court upheld the District Court's finding that a state may regulate the sale of material that is harmful to minors under the age of seventeen, even if not obscene by adult standards.[9] The New York statute in question prohibited material that "(i) predominantly appeals to the prurient, shameful, or morbid interest of minors, and (ii) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable materials for minors, and (iii) is utterly without redeeming social importance for minors."[10]

While the Supreme Court has upheld some laws that regulate indecent broadcasts on radio and television, the nature of the Internet is not analogous to radio and television, since it does not fall within the purview of any governmental regulatory

[7] Miller v. California, 413 U.S. 15, 18 (1973).
[8] *Id.* at 24.
[9] Ginsberg v. New York, 390 U.S. 629 (1968).
[10] *Id.* at 645-47.

agency.[11] In addition, because of its global reach, the Internet makes the application of the *Miller* and *Ginsberg* tests extremely difficult if not technologically impossible, at least for now. Internet sites can originate from servers anywhere in the world, making it virtually impossible for courts in the United States to enforce any legislation banning the publishing of certain material deemed harmful.

III. Congressional Attempts at Regulation

In trying to shield minors from the proliferation of pornographic material, Congress has made three attempts at regulating children's access to pornographic sites. These attempts include the Communications Decency Act, the Child Online Protection Act, and the Children's Internet Protection Act.

In 1996, Congress passed the Communications Decency Act (CDA),[12] which criminalized the knowing transmission of obscene or indecent communications to persons under the age of eighteen. The CDA prohibited "knowingly sending or displaying to a person under eighteen any message that, in context, depicts or describes, in terms patently offensive as measured by community standards, sexual or excretory activities or organs."[13] Affirmative

[11] *See* FCC v. Pacifica Found., 438 U.S. 726 (1978) (finding that the broadcast of indecent language at times of the day when children might be listening is inappropriate); Action for Children's Television v. FCC, 852 F.2d 1332 (1988) (upholding FCC regulation that only allowed the broadcasting of indecent material between midnight and 6:00 am). *But see* United States v. Playboy Entm't Group, Inc., 529 U.S. 803 (2000) (holding Telecommunications Act's "signal bleed" provision to scramble sexually explicit channels was not least restrictive means of protecting children).

[12] Communications Decency Act, 47 U.S.C. § 223 (2001).

[13] 47 U.S.C. § 223(d) (2001).

defenses were provided for those who took good faith, effective actions to restrict access by minors or for those who restricted access by requiring proof of age.[14] However, in *Reno v. ACLU*, the Supreme Court ruled that the CDA's content-based restrictions on speech were unconstitutional.[15] The Court was concerned that the unique nature of the Internet made age verification virtually impossible and that the content-based blanket restrictions on speech were overbroad and not narrowly tailored.[16]

In order to solve the problems with the CDA, in 1998 Congress passed the Child Online Protection Act (COPA).[17] COPA prohibits an individual or entity from "knowingly and with knowledge or the character of the material, in interstate or foreign commerce by means of the World Wide Web, making any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors."[18] In an effort to cure the constitutional problems with the CDA, Congress restricted the scope of COPA to material on the World Wide Web with a commercial purpose that was deemed harmful to minors.[19] COPA also provided an affirmative defense if, in good faith, the defendant has restricted access by minors to material that is harmful to minors "(1) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (2) by accepting a digital certificate that verifies age; or (3) by any

[14] 47 U.S.C. § 223(e)(5)(A)-(B) (2001).
[15] Reno v. ACLU, 521 U.S. 844 (1997).
[16] *Id.*
[17] 47 U.S.C. § 231 (2001).
[18] 47 U.S.C. § 231(a)(1) (2001).
[19] Reno v. ACLU, 217 F.3d 162, 167 (2000).

other reasonable measures that are feasible under available technology."[20]

The United States Court of Appeals for the Third Circuit declared COPA unconstitutional and issued a preliminary injunction preventing the enforcement of the Act.[21] Although the District Court for the Eastern District of Pennsylvania found that the Act was not narrowly tailored and imposed an excessive burden on Web publishers, the Court of Appeals based its decision solely on COPA's reliance on contemporary community standards to identify material that is harmful to minors, particularly as it relates to the Internet.[22] The Third Circuit focused on the aspect that the World Wide Web is not geographically constrained and that there is no technology currently available that would allow publishers to prevent their sites' content from entering a particular geographic area. As such, the community standards test would require every publisher to abide by the most restrictive communities' standards.[23] Adults in more liberal communities with less stringent standards would be denied the right to view material that was constitutionally protected because the publishers would be obligated to adhere to the standards of stricter communities. The Court of Appeals found this aspect of COPA to impose an overreaching burden on constitutionally protected speech and therefore declared the Act unconstitutional.[24]

[20] 47 U.S.C. § 231(c)(1)(A)-(C) (2001).
[21] *ACLU*, 217 F.3d at 166.
[22] *Id.* at 173.
[23] *Id.* at 175.
[24] *Id.* at 177.

In November 2001, the Supreme Court heard oral arguments regarding the federal constitutionality of COPA.[25] The Court's questions focused on exactly what Congress intended with its "community standards" test and whether Congress meant a community standard in the context of the Internet as a national standard.[26] Senator John McCain (R- Ariz.) and retired Representative Thomas Bliley (R-Va.) submitted a brief to the Court in which they stated:

> What is harmful to minors isn't decided by a geographical community. Instead it is based on the views of the American adult community as a whole. The law was to be adapted to the World Wide Web by using a new standard of what the American adult-age community as a whole would find prurient and offensive to minors.[27]

If the Supreme Court determines that the community standards test is based on some national standard, then the constitutionality of COPA will still be unclear since the Third Circuit would then need to address the other First Amendment concerns raised by the District Court.

Ironically, if the Supreme Court were to adopt this national standard it would undermine the *Ginsberg* and *Miller* tests. The Supreme Court stated in *Miller* that "our nation is simply too big and too diverse for this Court to reasonably expect that such

---

[25] Linda Greenhouse, *Justices Revisit the Issue of Child Protection in the Age of Internet Pornography*, N.Y. TIMES, Nov. 29, 2001, at A28.
[26] *Id.*
[27] Scott Ritter, *Court Weighs Shielding Children From Web Smut,* WALL ST. J., Nov. 26, 2001, at B14.

standards of what is patently offensive could be articulated for all fifty states in a single formulation."[28] However, the unique non-geographic nature of the Internet might make a national standard the only feasible alternative.

While Congress awaits the constitutional fate of COPA, they passed yet another measure to protect children from access to harmful material on the Internet. In 2001, Congress passed the Children's Internet Protection Act (CIPA).[29] CIPA requires that K-12 schools and public libraries that receive certain types of federal funding "(1) purchase and install technology protection measures that block or filter Internet access to certain, specified 'visual depictions,' (2) create Internet safety policies, and (3) conduct at least one public meeting to collect input from community members with a relationship to the school."[30] Visual depictions to be blocked or filtered include those that are obscene, child pornography and depictions that are deemed harmful to minors.[31] As with the Act's predecessors, the ACLU, along with the American Library Association, plan on bringing a lawsuit challenging the constitutionality of the filtering requirement of CIPA as a violation of the First Amendment's freedom of speech.[32] Congress will once again wait to hear from the Supreme Court whether or not its latest attempt to protect children from

[28] Miller v. California, 413 U.S. 15, 30 (1973).
[29] Kathleen Conn, *Protecting Children from the Internet Harm (Again): Will the Children's Internet Protection Act Survive Judicial Scrutiny?*, 153 Ed. L. Rep. (West) 469, 470 (2001).
[30] *Id.* at 473.
[31] *Id.*
[32] John Schwartz, *Internet Filters Used to Shield Minor Censor Speech, Critics Say*, N.Y. TIMES, Mar. 19, 2001, at A15.

pornography on the Internet can withstand a constitutional challenge.

IV. Why Is the Internet Technologically Difficult to Regulate?

To understand the Supreme Court's concern with the statutes that Congress has passed in an attempt to protect children, it is important to understand the unique nature of the Internet and why it is so difficult to regulate. The Internet functions as a global network connecting millions of computers around the world.[33] No one single organization or entity controls this network; instead it is a decentralized, self-maintained networking system that transmits communications by linking computers and computer networks around the world.[34] Within the Internet is the World Wide Web, which is a publishing forum consisting of individual formatted documents or 'websites' that contain text, images or sounds provided by that site's creator.[35] Web pages are made available to other users by connecting the publisher's computer to the Internet. Once this happens, an end user can move freely from one Web page to another by clicking on a link. Each site is connected to the Internet and becomes accessible to everyone on the Web anywhere in the world. The fact that there is no centralized point currently makes it impossible for websites or services to block the content of their pages from locations around the world.[36] In fact, a Web

[33] As of 1999 there were more than 200 million users of the Internet worldwide. Online computer dictionary for Internet Terms and Technical Support, *at* http://www.webopedia.com/TERM/I/Internet.html (last visited Oct. 14, 2001) (on file with the North Carolina Journal of Law & Technology).
[34] *Id.*
[35] ACLU v. Reno, 929 F. Supp. 824, 838 (1996).
[36] *Id.*

publisher has no way of knowing the geographic location of visitors to its site.[37]

The Supreme Court has been very clear that it is the technological aspects of the Internet that have made many of the regulations passed by Congress unconstitutional. As the Court stated:

> We are forced to recognize that, at present, due to technological limitations, there may be no other means by which harmful material on the Web may be constitutionally restricted, although, in light of rapidly developing technological advances, what may now be impossible to regulate constitutionally may, in the not-too-distant future, become feasible.[38]

The Court seems to believe that if technology ultimately allows the publishers to control access to their sites, Congress will be able to regulate them.

Some believe the movement toward a new national standard instead of community standards would solve many of the concerns over what type of material can be published. However, this approach ignores the global nature of the Internet. Web publishers fearful of prosecution for Web content access in the United States could easily move their sites to foreign servers. Europe is experiencing the same "global" problem with their attempts to criminalize speech on the Internet that they deem racist or xenophobic. A French court recently found Yahoo guilty of

---

[37] *Id.*

[38] ACLU v. Reno, 217 F.3d 162, 166 (2000).

violating France's speech laws by allowing pro-Nazi propaganda to be sold on its auction site.[39] However, the United States District Court for the Northern District of California held that European nations have no authority to regulate speech that originates in the United States.[40] The United States will have the same problem in its attempts to regulate harmful material that originates outside of the United States.

V. Is There a Technological Solution?

So, how do we protect children from pornography without violating free speech rights guaranteed in the First Amendment? The government certainly has a right to enact laws protecting children.[41] However, until the technological blocking concerns can be addressed, the answer might be found in personal responsibility and general market principles.

Many opponents of CDA, COPA, and CIPA argue that, instead of government regulation, parental monitoring of a child's Internet access and the use of filtering software to block access to certain sites will protect children. While these are valid solutions, they do not necessarily work. A recent study indicated that about half of parents do not supervise their children's Internet usage.[42] In addition, many children understand the Internet better than their parents, so supervision may be futile.

---

[39] Yahoo! Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (2001).

[40] *Id.*

[41] New York v. Ferber, 458 U.S. 747 (1982) (holding that a state has a compelling interest in protecting children).

[42] *See* Mike Snider, *Study: Kids Lacking Net Supervision*, USA TODAY, May 27, 1999, at B7.

Filtering software itself has run into constitutional challenges. In Loudon County, Virginia, the Federal District Court for the Eastern District of Virginia found mandatory filtering devices on library computers to be unconstitutional.[43] The Supreme Court has not ruled on the issue of mandatory filtering devices although the passage of CIPA might expedite a decision. Additionally, most filtering devices are textually based and screen out sites based on keywords and addresses.[44] The result is an over- and under-inclusive filtering device that often misses harmful material in the form of graphics and blocks valuable artistic, political or medical information because of the use of keywords.[45]

Another solution might be found in the creation of adult-oriented top-level domains (TLDs).[46] In layman terms, the TLD is the identifier that comes after the 'dot' in all Internet addresses. For instance, in the Internet address 'whitehouse.gov', 'whitehouse' is the second-level domain and 'gov' is the top-level domain. Originally designed and used by the military, the Internet

[43] Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library, 24 F. Supp. 2d 552 (1998) (holding the use of filtering software on a library computer violated the First Amendment).

[44] Patrick Poole, *The Online Decency Solution*, Covenant Syndicate, *at* http://capo.org/opeds/pp0709.html (last visited Sept. 15, 2001) (on file with the North Carolina Journal of Law & Technology).

[45] Declan McCullagh, *Anti-Porn Law Under Fire* (Sept. 1, 1999), *at* http:/www.wired.com/news/politics/0,1283,37996.2.00.html (on file with the North Carolina Journal of Law & Technology). Filtering software blocked the COPA Commission website because the biographical pages included the word "cum" in magna-cum-laude.

[46] Chris Stamper, *XXX Marks the Porn Site* (July 20, 1998), ABCNews, *at* http://www.more.abcnews.go.com/sections/tech/dailynews/dotxxx970715.html (on file with the North Carolina Journal of Law & Technology).

had very few computers connected to the network.[47] As such, each computer was identified and located by its own unique numeric address called an Internet protocol address (IP).[48] Each individual computer stored the addresses of the other computers so you could contact another computer by entering its unique address. An analogy to a phone directory is often used to describe this system.

However, as the number of computers and users grew, the system became burdensome. A new system was designed to respond to this growth using a hierarchical database structure, which allowed for top and second-level domain names.[49] The new system facilitates the use of easily-identified names that are then converted to numeric IP addresses so a particular item of information within the Web can be located.[50] Seven top-level domains such as ".gov," ".edu," and ".com" were created.[51] Second-level names are then registered under the top-level domains. It is within the top-level domain name system that a possible market solution might exist.

Although probably driven more by market forces than concern for children, several companies are now beginning to sell and market adult-themed domains. The credit card nature of most pornographic sites makes it advantageous to publishers to create adult-oriented domains.[52] Although the top-level domains are

---

[47] New.Net, A Proposal to Introduce Market-Based Principles into Domain Name Governance, *at* http://www.new.net (last visited on Sept. 22, 2001) (on file with the North Carolina Journal of Law & Technology).
[48] *Id.*
[49] Management of Internet Names and Addresses, 63 Fed. Reg. 31, 741-01 (1998).
[50] *Id.*
[51] *Id.*
[52] *See* Poole, *supra* note 44.

voluntary, Internet Service Providers (ISPs) may opt to force their registrants to operate under the new domain so they can market themselves as family friendly.[53] From the perspective concerning children, the new top-level domains such as ".xxx" or ".sex" would make it much easier for filtering devices to block pornographic materials. Instead of the keyword, the filtering device could focus on the site's top-level domain. If nothing else, it would make it easier and therefore maybe more likely for parents to identify and monitor the sites their children visit on the Web. They would know when their children had entered the 'red light district' of the Internet. Additionally, a majority of schools use filtering software; and, it is estimated that, by 2003, Internet access from school is expected to surpass access from home.[54] However, the creation of these new TLDs has created a stir within the Internet community since the companies marketing the new domains have circumvented the governing Internet body (ICANN) to create these domains.[55]

Originally, Network Solutions, Inc., was given authority to register second-level domains and administer the main root server known as the "A" root server.[56] However, once the marketplace recognized the commercial value of the Web, the number of users skyrocketed.[57] It became apparent that as the system continued to grow, there would need to be some sort of governing body to oversee the expansion of the Internet. The Department of

---

[53] *See* Stamper, *supra* note 46.
[54] *See* Grunwald Associates, *supra* note 5.
[55] Andy Patrizio, *New.net Defies Domain System* (Mar. 5, 2001), *at* http://www.wired.com/news/business/0,1367,42146,00.html (on file with the North Carolina Journal of Law & Technology).
[56] *Id.*
[57] *Id.*

Commerce issued a white paper calling for the creation of a not-for-profit corporation to administer the domain system.[58] As a result, the Internet Corporation for Assigned Names and Numbers (ICANN) was created to administer address names.[59] One of the first tasks of ICANN was to respond to the enormous demand and outcry for new top-level domains. In November 2000, ICANN approved seven new top-level domains even though they had received requests for more than forty.[60]

Since its inception, the Internet has functioned under a consensus approach. Technical issues have often been decided by bringing together various parties in the field from around the world to devise solutions to which all parties agreed to adhere.[61] It was assumed that ICANN's authority would stem from this consensus approach, but concerns over ICANN making policy instead of technical decisions have caused some entities within the Internet community to sidestep its decision-making authority, particularly with regard to new top-level domains.[62]

---

[58] Management of Internet Names and Addresses, 63 Fed. Reg. 31741 (June 10, 1998), *available at* 1998 WL 298883.

[59] ICANN Fact Sheet, *at* http://www.icann.org/general/fact-sheet.htm (last visited Mar. 14, 2002) (on file with the North Carolina Journal of Law & Technology). ICANN was created in 1998 by a coalition of the Internet's business, technical, academic and user communities. Its primary function is to coordinate the assignment of address identifiers as well as the operation of the root server system.

[60] Declan McCullagh and Ryan Sager, *Getting to Domain Argument* (Feb. 8, 2001), *at* http://wired.com/news/politics/0,1283,41683,00.html (on file with the North Carolina Journal of Law & Technology). New TLD's are .aero, .biz, .coop, .info, .museum, .name, and .pro.

[61] New.net, A Proposal to Introduce Market-Based Principles into Domain Name Governance, *supra* note 47.

[62] *Id.*

One such company, New.net, began offering twenty new top-level domains, none of which were approved by ICANN.[63] Realizing the advantage of adult-oriented top-level domains, New.net created a new domain called ".xxx."[64] The creation of a TLD outside of ICANN does pose some technical problems with regard to routing.[65] Because the New.net domains are outside of the ICANN system, customers are limited to two possible ways of accessing the sites with the new TLDs. Only customers of ISPs who have partnered with New.net can access the sites. However, if a service provider has not partnered with New.net, individuals have the option of downloading a plug-in program so their browsers can access the new sites.[66] Earthlink, Excite, and NetZero have agreed to partner with New.net, which means New.net can reach close to forty-two million users.[67]

New.net is not the only company interested in adult domains. Domain Name Systems, another company who has worked closely with the porn industry, has also begun offering .xxx names.[68] Additionally, ICM Registry is a company that

---

[63] *See* Patrizio, *supra* note 55.

[64] Andy Patrizio, *XXX Domain May Be Hard to Sell* (Mar. 6, 2001), *at* http://www.wired.com/news/business/0,1367,42217,00.html (on file with the North Carolina Journal of Law & Technology).

[65] *See* Patrizio, *supra* note 55. These TLDs require the reconfiguration of DNS servers that turn words into numeric IP Addresses.

[66] *See id.*

[67] Ben Fritz, *In Dueling Proposals, ICANN and New.net Face Off on the Role of Market Forces in Regulating the Internet, at* http://www.new.net/news_release_11.tp (last visited Mar. 15, 2002) (on file with the North Carolina Journal of Law & Technology).

[68] Andy Patrizio, *Confusion Is Domain Problem* (Mar. 14, 2001), *at* http://wired.com/news/business/0,1367,42373,00.html (on file with the North Carolina Journal of Law & Technology).

actually submitted a .xxx domain proposal to ICANN and, although it was not initially approved, is still lobbying to get the domain approved by ICANN.[69]

The result of multiple companies registering second-level domains under the same top-level domain names creates both technical and legal problems.[70] In the past, the second-level domain names that were registered were easily managed since the companies registering the second-level domains had control of the top-level domain. But now, one company could register 'girls.xxx' with one company and someone else could register 'girls.xxx' with a different company.[71] When a user types 'girls.xxx', to whose site will the user be routed and who has a legal claim to that site's name?

In 1999, ICANN adopted the Uniform Domain Name Dispute Resolution Process to deal with disputes regarding conflicting claims over identical or similarly named sites.[72] Anyone who is approved by ICANN must agree to have any disputes handled through this resolution process.[73] But if the new top-level domains are created outside the authority of ICANN, then the companies registering under these new domains are not bound by any of ICANN's policies. And since ICANN's authority stems

---

[69] *Id.*

[70] *See id.*

[71] *See id.* There is little copyright law governing TLDs; it is unclear who would have a legal right to the domain.

[72] Oscar Cisneros, *What to do with Domain Disputes* (Nov. 13, 2000), *at* http://www.wired.com/news/politics/0,1283,39993,00.html (on file with the North Carolina Journal of Law & Technology).

[73] *ICANN Frequently Asked Questions, available at* http://www.icann.org/general/faq1.html (last visited Feb. 8, 2002) (on file with the North Carolina Journal of Law & Technology).

from consensus, they have no real power to stop these companies from creating these domains.

So, what happens if multiple companies register duplicate names with companies offering the TLDs outside of ICANN? Users could end up at different sites depending on their browser or their ISP. For instance, Earthlink is currently partnered with New.net, so if the user typed in 'girls.xxx', the user would end up at the site registered with New.net. However, if the user accessed the site from a different computer with a different ISP, and there is a duplicate site registered with another company like Domain Name Systems, the user would end up at that alternative site.[74]

Under current trademark guidelines, companies or individuals applying for trademark protection for top-level domains are denied.[75] One of the key components of obtaining a trademark or service mark for a domain name is that it indicates the source to a website customer. This is why the courts and the trademark office have traditionally focused on the second-level domain name as opposed to the beginning of the address such as "http://www" or the top-level domain such as ".com". This policy was evident in a recent court case where an TLD operator seeking

[74] *See* Patrizio, *supra* note 68.

[75] U.S. Department of Commerce, Patent and Trademark Office, *Examination Guide No. 2-99 Marks Composed, in Whole or in Part, of Domain Names* (Sept. 29, 1999), *at* http://www.uspto.gov/web/offices/tac/notices/guide299.htm (on file with the North Carolina Journal of Law & Technology) (Determining that if a mark is composed solely of TLD for domain name registry services, registration should be refused under the Trademark Act on the ground that the TLD would not be perceived as a mark).

a trademark for the unofficial top-level domain ".web" lost its bid.[76]

Unfortunately, the legal confusion surrounding the new top-level domains and the concern over who will ultimately hold the rights to a particular name or site could prevent providers of pornography from taking advantage of the new adult-oriented top-level domains. However, if ICANN were to approve an adult-oriented top-level domain and companies like New.net were willing to fall under the authority of ICANN, then the chances of the adult-oriented sites being successful would be much stronger.

VI. Conclusion

Very few people disagree that children should be protected from viewing harmful material on the Internet. Congress's effort to pass an effective online obscenity law with COPA is being tested today, and we await the United Stated Supreme Court's decision. The global nature of the Internet and technological infeasibilities of blocking end-user access to particular sites create valid constitutional First Amendment concerns. And while Congress has the authority to regulate obscene material until the technological hurdles can be overcome, statutory solutions will not be able to prevent children from accessing harmful sites. Instead of new laws, market solutions might be more effective at controlling children's access to pornography.

Partial solutions are available in parental monitoring and filtering devices, but the most effective tool might be the creation

[76] Oscar Cisneros, *Some Dots Can't Be Trademarked* (Sept. 18, 2000), *at* http://www.wired.com/news/politics/0,1283,38836,00.html (on file with the North Carolina Journal of Law & Technology).

of a 'red light district' within the Internet through the use of adult-oriented top-level domains. Because the Internet is not controlled by any government entity and website publishers and providers cannot be forced to use the new top-level domains, the success of these new domains will depend on general market forces. Another important factor in the new domains' ultimate success will be resolution on many of the legal concerns surrounding ownership of the various sites. In the meantime, those pornographers that have voluntarily decided to use the new adult-oriented top-level domains have done a service to children since it is easier to block top-level domains.